

ESET MAIL SECURITY

PARA MICROSOFT EXCHANGE SERVER

Manual de instalación y guía para el usuario

Microsoft® Windows® Server 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

[Haga clic aquí para mostrar la versión de ayuda en línea de este documento](#)

ESET MAIL SECURITY

Copyright ©2016 por ESET, spol. s r.o.

ESET Mail Security fue desarrollado por ESET, spol. s r.o.

Para obtener más información, visite www.eset-la.com.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o medio alguno, ya sea electrónico, mecánico, fotocopia, grabación, escaneo o cualquier otro medio sin la previa autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier elemento del software de la aplicación sin previo aviso.

Atención al cliente: www.eset.com/support

REVISADO EN 28/11/2016

Contenido

1. Introducción.....	6
1.1 Novedades.....	6
1.2 Páginas de ayuda.....	7
1.3 Métodos usados.....	8
1.3.1 Protección de la base de datos del buzón de correo electrónico.....	9
1.3.2 Protección del transporte de correo electrónico.....	9
1.3.3 Exploración de la base de datos a petición.....	9
1.4 Tipos de protección.....	11
1.4.1 Protección antivirus.....	11
1.4.2 Protección antispam.....	11
1.4.3 Aplicación de reglas definidas por el usuario.....	11
1.5 Interfaz del usuario.....	12
1.6 Requisitos del sistema.....	13
1.6.1 ESET Mail Security características y roles de Exchange Server.....	14
1.6.1.1 Roles de Exchange Server: comparación de Edge y Hub.....	15
1.6.1.2 Roles de Exchange Server 2013.....	16
1.7 Administrado a través de ESET Remote Administrator.....	16
2. Instalación.....	18
2.1 ESET Mail Security pasos de instalación.....	19
2.1.1 Instalación de la línea de comandos.....	22
2.1.2 Instalación en un entorno de clúster.....	24
2.2 Activación del producto.....	25
2.3 Terminal Server.....	26
2.4 ESET AV Remover.....	27
2.5 Conector y antispam POP3.....	27
2.6 Reemplazo por una versión más nueva.....	28
2.6.1 Actualización mediante ERA.....	29
2.6.2 Actualización mediante el clúster de ESET.....	31
3. Guía para principiantes.....	35
3.1 Supervisión.....	35
3.2 Archivos de registro.....	37
3.2.1 Registro de exploración.....	40
3.3 Exploración.....	42
3.3.1 Exploración de Hyper-V.....	44
3.4 Cuarentena de correo.....	46
3.4.1 Detalles del correo en cuarentena.....	48
3.5 Actualización.....	49
3.5.1 Configurar la actualización de DB de virus.....	51
3.5.2 Configurar el servidor proxy para actualizaciones.....	53
3.6 Configuración.....	54
3.6.1 Servidor.....	55
3.6.2 Equipo.....	56
3.6.3 Herramientas.....	58
3.6.4 Importación y exportación de una configuración.....	59
3.7 Herramientas.....	60

3.7.1	Procesos activos	61
3.7.2	Observar la actividad	63
3.7.2.1	Selección del período de tiempo	64
3.7.3	Estadísticas de la protección.....	64
3.7.4	Cluster	65
3.7.4.1	Asistente de clúster: página 1	67
3.7.4.2	Asistente de clúster: página 2	69
3.7.4.3	Asistente de clúster: página 3	70
3.7.4.4	Asistente de clúster: página 4	72
3.7.5	Shell de ESET.....	75
3.7.5.1	Uso.....	77
3.7.5.2	Comandos.....	81
3.7.5.3	Archivos por lotes/ Cifrado	83
3.7.6	ESET SysInspector	84
3.7.6.1	Creación de una instantánea de estado del equipo.....	84
3.7.6.2	ESET SysInspector	84
3.7.6.2.1	Introducción a ESET SysInspector.....	84
3.7.6.2.1.1	Inicio de ESET SysInspector	85
3.7.6.2.2	Interfaz del usuario y uso de la aplicación	85
3.7.6.2.2.1	Controles de programa.....	85
3.7.6.2.2.2	Navegación por ESET SysInspector	87
3.7.6.2.2.1	Accesos directos desde el teclado.....	88
3.7.6.2.2.3	Comparación.....	89
3.7.6.2.3	Parámetros de la línea de comandos	90
3.7.6.2.4	Script de servicio.....	91
3.7.6.2.4.1	Generación de scripts de servicio.....	91
3.7.6.2.4.2	Estructura del script de servicio	91
3.7.6.2.4.3	Ejecución de scripts de servicio.....	94
3.7.6.2.5	Preguntas frecuentes.....	94
3.7.6.2.6	ESET SysInspector como parte de ESET Mail Security.....	96
3.7.7	ESET SysRescue Live.....	96
3.7.8	Programador.....	96
3.7.8.1	Programador: agregar tarea	98
3.7.9	Enviar muestras para su análisis.....	99
3.7.9.1	Archivo sospechoso.....	99
3.7.9.2	Sitio sospechoso	100
3.7.9.3	Archivo falso positivo	100
3.7.9.4	Sitio falso positivo.....	100
3.7.9.5	Otros.....	100
3.7.10	Cuarentena.....	101
Ayuda y soporte.....		102
3.8.1	Cómo.....	102
3.8.1.1	Cómo actualizar ESET Mail Security.....	103
3.8.1.2	Cómo activar ESET Mail Security.....	103
3.8.1.3	Cómo ESET Mail Security cuenta los buzones de correo	104
3.8.1.4	Cómo crear una nueva tarea en Tareas programadas..	104
3.8.1.5	Cómo programar una tarea de exploración (cada 24 horas).....	105
3.8.1.6	Cómo quitar un virus del servidor.....	105
3.8.2	Enviar una solicitud de soporte	105
3.8.3	Limpiador especializado de ESET	106
3.8.4	Acerca de ESET Mail Security.....	106

3.8.5	Activación del producto	106
3.8.5.1	Registro	107
3.8.5.2	Activación de Security Admin	107
3.8.5.3	Falla en la activación	107
3.8.5.4	Licencia	108
3.8.5.5	Progreso de la activación	108
3.8.5.6	La activación se completó correctamente	108

4. Trabajo con ESET Mail Security.....109

4.1 Servidor.....110

4.1.1	Configuración de la prioridad del agente	111
4.1.1.1	Modificar prioridad	111
4.1.2	Configuración de la prioridad del agente	111
4.1.3	Antivirus y antispyware	112
4.1.4	Protección antispam	113
4.1.4.1	Filtro y verificación	114
4.1.4.2	Configuración avanzada	115
4.1.4.3	Configuración de la lista gris	119
4.1.4.4	SPF y DKIM	121
4.1.5	Reglas	122
4.1.5.1	Lista de reglas	122
4.1.5.1.1	Asistente de reglas	123
4.1.5.1.1.1	Condición de regla	124
4.1.5.1.1.2	Acción de regla	126
4.1.6	Protección del transporte de correo electrónico	128
4.1.6.1	Configuración avanzada	130
4.1.7	Protección de la base de datos del buzón de correo electrónico	131
4.1.8	Exploración de la base de datos a petición	132
4.1.8.1	Elementos adicionales del buzón de correo	134
4.1.8.2	Servidor proxy	134
4.1.8.3	Detalles de la cuenta de la exploración de la base de datos	135
4.1.9	Cuarentena de correo	136
4.1.9.1	Cuarentena local	137
4.1.9.1.1	Almacenamiento de archivos	138
4.1.9.1.2	Interfaz Web	139
4.1.9.2	Buzón de correo de cuarentena y cuarentena de MS Exchange	144
4.1.9.2.1	Configuración de la administración de cuarentena	144
4.1.9.2.2	Servidor proxy	145
4.1.9.3	Detalles de la cuenta del administrador de la cuarentena	146

4.2 Equipo.....146

4.2.1	Detección de una infiltración	147
4.2.2	Exclusiones de procesos	148
4.2.3	Exclusiones automáticas	149
4.2.4	Caché local compartido	149
4.2.5	Rendimiento	150
4.2.6	Protección del sistema de archivos en tiempo real	150
4.2.6.1	Exclusiones	151
4.2.6.1.1	Agregar o editar exclusiones	152
4.2.6.1.2	Formato de las exclusiones	153

4.2.6.2	ThreatSense parámetros	153
4.2.6.2.1	Extensiones de archivos que no se analizarán	156
4.2.6.2.2	Parámetros ThreatSense adicionales	157
4.2.6.2.3	Niveles de desinfección	157
4.2.6.2.4	Cuándo modificar la configuración de la protección en tiempo real	158
4.2.6.2.5	Verificación de la protección en tiempo real	158
4.2.6.2.6	Qué hacer si la protección en tiempo real no funciona	158
4.2.6.2.7	Envío	158
4.2.6.2.8	Estadísticas	159
4.2.6.2.9	Archivos sospechosos	159
4.2.7	Exploración del equipo y exploración de Hyper-V a petición	160
4.2.7.1	Ejecución de la exploración personalizada y exploración Hyper-V	160
4.2.7.2	Progreso de la exploración	163
4.2.7.3	Administrador de perfiles	164
4.2.7.4	Objetos para explorar	165
4.2.7.5	Pausar la exploración programada	165
4.2.8	Exploración en estado inactivo	165
4.2.9	Exploración en el inicio	166
4.2.9.1	Verificación de archivos de inicio automática	166
4.2.10	Medios extraíbles	167
4.2.11	Protección de documentos	167
4.2.12	HIPS	167
4.2.12.1	Reglas HIPS	169
4.2.12.1.1	Configuración de reglas HIPS	170
4.2.12.2	Configuración avanzada	172
4.2.12.2.1	Controladores siempre permitidos para cargar	172

4.3 Actualización.....172

4.3.1	Revertir actualización	174
4.3.2	Modo de actualización	174
4.3.3	Proxy HTTP	175
4.3.4	Conectarse a la LAN como	176
4.3.5	Mirror	177
4.3.5.1	Actualización desde el mirror	179
4.3.5.2	Archivos espejo	181
4.3.5.3	Resolución de problemas de actualización desde el mirror	181
4.3.6	Cómo crear tareas de actualización	182

4.4 Internet y correo electrónico.....182

4.4.1	Filtrado de protocolos	182
4.4.1.1	Aplicaciones excluidas	183
4.4.1.2	Direcciones IP excluidas	183
4.4.1.3	Clientes de Internet y correo electrónico	183
4.4.2	SSL/TLS	183
4.4.2.1	Comunicación cifrada SSL	185
4.4.2.2	Lista de certificados conocidos	186
4.4.3	Protección del cliente de correo electrónico	186
4.4.3.1	Protocolos de correo electrónico	187
4.4.3.2	Alertas y notificaciones	187
4.4.3.3	Barra de herramientas de MS Outlook	188

Contenido

4.4.3.4	Barra de herramientas de Outlook Express y Windows Mail	188	4.10	Programador	221
4.4.3.5	Cuadro de diálogo de confirmación	189	4.10.1	Detalles de tarea	223
4.4.3.6	Exploración reiterada de los mensajes	189	4.10.2	Programación de tareas: única vez	223
4.4.4	Protección del acceso a la Web	189	4.10.3	Programación de tarea	223
4.4.4.1	Básico	190	4.10.4	Programación de tareas: a diario	224
4.4.4.2	Administración de direcciones URL	190	4.10.5	Programación de tareas: semanalmente	224
4.4.4.2.1	Creación de una nueva lista	191	4.10.6	Programación de tareas: accionada por suceso	224
4.4.4.2.2	Lista de direcciones	191	4.10.7	Detalles de la tarea: lanzar la aplicación	224
4.4.5	Protección Anti-Phishing	192	4.10.8	Detalles de la tarea: enviar informes de cuarentena de correo	224
4.5	Control del dispositivo	194	4.10.9	Pasar por alto tarea	225
4.5.1	Control del dispositivo: editor de reglas	195	4.10.10	Resumen general de tareas programadas	225
4.5.2	Agregado de reglas del control del dispositivo	196	4.10.11	Tareas del programador: exploración en segundo plano	225
4.5.3	Dispositivos detectados	197	4.10.12	Perfiles de actualización	226
4.5.4	Grupos de dispositivos	198	4.11	Cuarentena	226
4.6	Herramientas	198	4.11.1	Envío de archivos a cuarentena	226
4.6.1	ESET LiveGrid	199	4.11.2	Restauración desde cuarentena	227
4.6.1.1	Filtro de exclusión	200	4.11.3	Envío de archivos desde cuarentena	227
4.6.2	Cuarentena	200	4.12	Actualizaciones del sistema operativo	227
4.6.3	Actualización de Microsoft Windows	200	5	Glosario	228
4.6.4	Proveedor WMI	200	5.1	Tipos de infiltraciones	228
4.6.4.1	Datos proporcionados	201	5.1.1	Virus	228
4.6.4.2	Acceso a los datos proporcionados	205	5.1.2	Gusanos	228
4.6.5	Objetivos para explorar de ERA	205	5.1.3	Trojanos	229
4.6.6	Archivos de registro	205	5.1.4	Rootkits	229
4.6.6.1	Filtrado de registros	207	5.1.5	Adware	229
4.6.6.2	Búsqueda en el registro	207	5.1.6	Spyware	230
4.6.7	Servidor proxy	208	5.1.7	Empaquetadores	230
4.6.8	Notificaciones por correo electrónico	209	5.1.8	Bloqueador de exploits	230
4.6.8.1	Formato de mensajes	210	5.1.9	Exploración de memoria avanzada	231
4.6.9	Modo presentación	210	5.1.10	Aplicaciones potencialmente no seguras	231
4.6.10	Diagnósticos	211	5.1.11	Aplicaciones potencialmente no deseadas	231
4.6.11	Atención al cliente	211	5.2	Correo electrónico	231
4.6.12	Cluster	212	5.2.1	Anuncios	232
4.7	Interfaz del usuario	213	5.2.2	Mensajes falsos	232
4.7.1	Alertas y notificaciones	215	5.2.3	Phishing	232
4.7.2	Configuración del acceso	216	5.2.4	Reconocimiento de fraudes de spam	233
4.7.2.1	Contraseña	217	5.2.4.1	Reglas	233
4.7.2.2	Configuración de la contraseña	217	5.2.4.2	Filtro bayesiano	233
4.7.3	Ayuda	217	5.2.4.3	Lista blanca	234
4.7.4	Shell de ESET	217	5.2.4.4	Lista negra	234
4.7.5	Deshabilitación de la interfaz gráfica del usuario en Terminal Server	218	5.2.4.5	Control desde el servidor	234
4.7.6	Mensajes y estados deshabilitados	218			
4.7.6.1	Mensajes de confirmación	218			
4.7.6.2	Estados de aplicaciones deshabilitados	218			
4.7.7	Ícono de la bandeja del sistema	219			
4.7.7.1	Detener protección	220			
4.7.8	Menú contextual	220			
4.8	Revertir toda la configuración en esta sección	221			
4.9	Revertir a la configuración predeterminada	221			

1. Introducción

ESET Mail Security 6 para Microsoft Exchange Server es una solución integrada que protege los buzones de correo ante diversos tipos de contenido malintencionado, incluyendo archivos adjuntos de correo electrónico infectados por gusanos o troyanos, documentos que contienen scripts dañinos, esquemas de phishing y spam. ESET Mail Security proporciona tres tipos de protección: antivirus, antispam y reglas definidas por el usuario. ESET Mail Security filtra el contenido malintencionado en el nivel del servidor de correo, antes de que llegue al buzón de entrada del destinatario.

ESET Mail Security es compatible con la versión 2003 de Microsoft Exchange Server y versiones posteriores, además de Microsoft Exchange Server en un entorno de clúster. En las versiones más nuevas (Microsoft Exchange Server 2003 y posteriores), los roles específicos (buzón de correo, concentradores, perimetral) son compatibles. En redes más grandes, es posible administrar ESET Mail Security en forma remota con la ayuda de [ESET Remote Administrator](#).

A la vez que proporciona protección para Microsoft Exchange Server, ESET Mail Security también incluye las herramientas para asegurar la protección del servidor en sí mismo (escudo residente, protección de acceso a la Web y protección del cliente de correo electrónico).

1.1 Novedades

- [Administrador de la cuarentena de correo](#): el administrador puede inspeccionar objetos en esta sección de almacenamiento y decidir si los eliminará o los liberará. Esta característica ofrece una administración sencilla de los correos electrónicos puestos en cuarentena por el agente de transporte.
- [Interfaz web de cuarentena de correo](#): una alternativa al administrador de cuarentena de correo basada en web.
- [Antispam](#): este componente esencial recibió un importante rediseño y ahora utiliza un nuevo motor galardonado con rendimiento mejorado. Validación de mensajes con [SPF y DKIM](#).
- [Exploración de la base de datos a petición](#): la exploración de la base de datos a petición utiliza el API de EWS (Servicios web de Exchange) para conectarse a Microsoft Exchange Server mediante HTTP/HTTPS. También, el explorador realiza exploración paralela para mejorar el rendimiento.
- [Reglas](#): el elemento del menú Reglas permite a los administradores definir manualmente las condiciones de filtrado de correo electrónico y las acciones a tomar con los mensajes de correo electrónico filtrados. Las reglas en la última versión de ESET Mail Security se diseñaron para otorgar mayor flexibilidad y dar al usuario aún más posibilidades.
- [Clúster de ESET](#): similar a ESET File Security 6 para Microsoft Windows Server, la unión de las estaciones de trabajo a nodos ofrecerá una automatización adicional de la administración debida a la posibilidad de distribuir una directiva de configuración entre todos los miembros del clúster. La creación de los clústeres mismos es posible mediante el nodo instalado, que luego podrá instalar e iniciar todos los nodos de manera remota. Los productos del servidor de ESET pueden comunicarse entre sí e intercambiar información, como la configuración y las notificaciones, y pueden [Sincronizar las bases de datos de la lista gris](#) además de sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias de productos. Esto permite tener la misma configuración del producto para todos los miembros de un clúster. ESET Mail Security es compatible con los clústeres de Windows Failover y de Network Load Balancing (NLB). Además, puede agregar miembros de clúster de ESET de forma manual sin necesidad de un clúster de Windows específico. Los clústeres de ESET trabajan en entornos de dominio y de grupo de trabajo.
- [Exploración de almacenamiento](#): explora todos los archivos compartidos en un servidor local. Esto hace que sea más fácil explorar de manera selectiva solamente los datos del usuario que se almacenan en el servidor de archivos.
- [Instalación basada en componentes](#): puede elegir los componentes desea añadir o eliminar.
- [Exclusiones de procesos](#): excluye procesos específicos de la exploración siempre activa del Antivirus. Debido al rol crítico de los servidores dedicados (servidor de aplicación, servidor de almacenamiento, etc.) las copias de respaldo periódicas son obligatorias para garantizar la recuperación oportuna de incidentes fatales de cualquier


tipo. Para mejorar la velocidad de las copias de respaldo, la integridad del proceso y la disponibilidad del servicio, durante las copias de respaldo se utilizan algunas técnicas que son conocidas por entrar en conflicto con la protección del antivirus a nivel del archivo. Pueden ocurrir problemas similares cuando se intentan realizar migraciones en vivo en máquinas virtuales. La única manera efectiva de evitar ambas situaciones es desactivar el software antivirus. Al excluir los procesos específicos (por ejemplo aquellos de la solución de copias de respaldo) todas las operaciones de archivos atribuidas a dichos procesos excluidos se ignorarán y se considerarán seguras, minimizando de esta manera la interferencia con los procesos de copia de respaldo. Le recomendamos que tenga precaución cuando cree exclusiones; una herramienta de copia de respaldo que haya sido excluida podrá acceder a los archivos infectados sin activar una alerta, motivo por el cual los permisos extendidos solamente se permiten en el módulo de protección en tiempo real.

- [eShell](#) (Shell de ESET): eShell 2.0 ahora está disponible en ESET Mail Security. eShell es una interfaz de línea de comandos que ofrece a los usuarios y administradores avanzados opciones más exhaustivas para administrar los productos de servidor de ESET.
- [Exploración de Hyper-V](#): es una nueva tecnología que permite explorar los discos de las máquinas virtuales (VM) en [Microsoft Hyper-V Server](#) sin la necesidad de tener instalado un “agente” en la VM en cuestión.
- Mejor integración con [ESET Remote Administrator](#) incluida la posibilidad de programar la [Exploración a petición](#).


1.2 Páginas de ayuda

El propósito de esta guía es ayudarlo a sacar el mayor provecho de ESET Mail Security. Para obtener más información sobre las ventanas del programa, presione la tecla F1 de su teclado mientras tiene abierta la ventana correspondiente. Se mostrará la página de ayuda correspondiente a la ventana que está viendo actualmente.


A fin de garantizar la consistencia y ayudar a evitar la confusión, la terminología que se usa en esta guía se basa en los nombres de parámetros de ESET Mail Security. También usamos un conjunto uniforme de símbolos para resaltar temas de interés o importancia en particular.


NOTA

Una nota es una observación breve. Aunque puede omitirlas, las notas pueden proporcionar información valiosa, tales como características específicas o un enlace a un tema relacionado.


IMPORTANTE

Es algo que requiere su atención y no recomendamos dejarlo de lado. En general, brinda información no crítica pero importante.


ADVERTENCIA

Debe tratar la información crítica con mayor cuidado. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente perjudiciales. Lea y comprenda el texto entre paréntesis de advertencia, ya que hace referencia a configuraciones del sistema altamente sensibles o a algo arriesgado.

Convención	Significado
En negrita	Nombres de elementos de interfaces como cuadros y botones de opciones.
<i>En cursiva</i>	Marcador de posición para la información que proporciona. Por ejemplo, <i>nombre de archivo</i> o <i>ruta</i> significa que debe escribir esa ruta o ese nombre de archivo.
Courier New	Comandos o ejemplos de códigos
Hipervínculo	Proporciona un acceso fácil y rápido a temas con referencias cruzadas o a ubicaciones de la web externa. Los hipervínculos están resaltados en azul y pueden estar subrayados.
%ProgramFiles%	Directorio del sistema Windows que almacena programas instalados de Windows y otros.

- Los temas de esta guía se dividen en varios capítulos y subcapítulos. Puede encontrar información relevante si explora en **Contenidos** en las páginas de ayuda. Como alternativa, puede usar el **Índice** para explorar por palabra clave o usar **Buscar** para el texto completo.

[Contents](#) | [Index](#) | [Search](#)

Enter one or more keywords to search (**
and '?' wildcards are supported):

Results per page: 10 ▼

Match: ☐ any search words ☒ all search words

ESET Mail Security le permite buscar los temas de ayuda por palabra clave o mediante la escritura de palabras o frases para buscar dentro de la Guía del usuario. La diferencia entre ambos métodos es que una palabra clave puede estar lógicamente relacionada con las páginas de Ayuda que no contienen esa palabra clave específica en el texto. La búsqueda por palabras y frases buscará el contenido de todas las páginas y mostrará solo aquellas que contengan la palabra o frase en el texto real.

- Puede publicar su calificación o enviar comentarios sobre un tema en particular en ayuda, haga clic en el enlace **¿Le resultó útil la información?** o **Califique este artículo: Útil / No útil** en el caso de la base de conocimiento de ESET, debajo de la página de ayuda.

1.3 Métodos usados

Los siguientes tres métodos se utilizan para explorar los correos electrónicos:

- [Protección de la base de datos de correo electrónico](#), anteriormente conocida como exploración de correo electrónico mediante VSAPI. Este tipo de protección solamente está disponible para Microsoft Exchange Server 2010, 2007 y 2003 que funciona en rol de Servidor del buzón de correo (Microsoft Exchange 2010 y 2007) o Servidor back-end (Microsoft Exchange 2003). Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya el rol de Casilla de correo o Respaldo).
- [Protección del transporte de correo](#), anteriormente conocida como Filtrado de mensajes al nivel del servidor SMTP. Esta protección es proporcionada por el agente de transporte y solo está disponible para Microsoft Exchange Server 2007 o más reciente ejecutado en rol de servidor Transporte Edge o servidor Transporte Hub. Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados).
- [Exploración de la base de datos a petición](#): le permite ejecutar o programar una exploración de la base de datos del buzón de correo Exchange. Esta característica solo está disponible para Microsoft Exchange Server 2007 o más reciente que funcione en el rol de Servidor de la casilla de correo o Transporte Hub. Esto también se aplica a una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados). Consulte [roles de Exchange Server 2013](#) para conocer algunos aspectos específicos acerca de los roles en Exchange 2013.

1.3.1 Protección de la base de datos del buzón de correo electrónico

Microsoft Exchange Server activa el proceso de exploración del buzón de correo y lo controla. Los correos electrónicos en el almacén de Microsoft Exchange Server se exploran constantemente. Dependiendo de la versión de Microsoft Exchange Server, la versión de la interfaz VSAPI y la configuración definida por el usuario, el proceso de exploración puede activarse en cualquiera de las siguientes situaciones:

- Cuando el usuario accede al correo electrónico, por ejemplo, en un cliente de correo electrónico (el correo electrónico siempre se explora con la última base de datos de firmas de virus)
- En segundo plano, cuando el uso de Microsoft Exchange Server es bajo
- En forma proactiva (basándose en el algoritmo interno de Microsoft Exchange Server)

Actualmente, la exploración antivirus y la protección basada en reglas utilizan la interfaz VSAPI.

1.3.2 Protección del transporte de correo electrónico

El filtrado en el nivel del servidor SMTP se asegura mediante el uso de un complemento especial. En Microsoft Exchange Server 2000 y 2003, el complemento en cuestión (Receptor de sucesos) se registra en el servidor SMTP como parte de Internet Information Services (IIS). En Microsoft Exchange Server 2007/2010, el complemento se registra como un agente de transporte en el rol Edge o Hub de Microsoft Exchange Server.

El filtrado en el nivel del servidor SMTP por un agente de transporte ofrece protección antivirus, antispam y mediante reglas definidas por el usuario. A diferencia del filtrado de VSAPI, el filtrado en el nivel del servidor SMTP se realiza antes de que el correo electrónico explorado llegue al buzón de correo de Microsoft Exchange Server.

1.3.3 Exploración de la base de datos a petición

Como ejecutar una exploración completa de la base de datos de correo electrónico en entornos grandes puede provocar una carga no deseada del sistema, puede elegir qué bases de datos y qué casillas de correo se explorarán allí dentro. Puede filtrar los objetivos de exploración en mayor medida al especificar la estampa de tiempo de los mensajes a explorar para minimizar el impacto sobre los recursos del sistema del servidor.

Los siguientes tipos de elementos se escanean tanto en Carpetas públicas como en Casillas de correo del usuario:

- Correo electrónico
- Publicar
- Elementos del calendario (reuniones/citas)
- Tareas
- Contactos
- Diario

1. Puede utilizar la lista desplegable para elegir qué mensajes explorar según la marca de tiempo. Por ejemplo, los mensajes modificados en la última semana. También puede elegir explorar todos los mensajes si es necesario.
2. Seleccione la casilla de verificación junto a **Explorar cuerpos del mensaje** para habilitar o deshabilitar la exploración del cuerpo del mensaje.
3. Haga clic en **Editar** para seleccionar la carpeta pública que se explorará.

Explorar mensajes modificados dentro de la última semana ▼

☒ Explorar cuerpos de mensaje

Carpetas públicas

..... Carpetas públicas /todas

Editar...

Casillas de correo electrónico

..... Servidores

..... Casillas de correo electrónico

Editar...

Guardar ⓘ

Aceptar Cancelar

4. Seleccione las casillas de verificación junto a las Bases de datos y Casillas de correo del servidor que desee explorar. El **Filtro** le permite encontrar las Bases de datos y las Casillas de correo rápidamente, en especial si existe una gran cantidad de casillas de correo en su infraestructura de Exchange.

Filtrar:

..... ⓘ

☒ Casillas de correo electrónico

☒ Users

☒ Administrator@franto.com

☒ user10@franto.com

☒ user1@franto.com

☒ user2@franto.com

☒ user3@franto.com

☒ user4@franto.com

☒ user5@franto.com

☒ user6@franto.com

☒ user7@franto.com

☒ user8@franto.com

☒ user9@franto.com

Aceptar Cancelar

5. Haga clic en **Guardar** los objetivos de exploración y los parámetros en el perfil de exploración a petición.

1.4 Tipos de protección

Existen tres tipos de protección:

- [Protección antivirus](#)
- [Protección antispam](#)
- [Aplicación de reglas definidas por el usuario](#)

1.4.1 Protección antivirus

La protección antivirus es una de las funciones básicas del producto ESET Mail Security. La protección antivirus defiende el sistema ante ataques malintencionados mediante el control de archivos, correos electrónicos y comunicaciones por Internet. Si se detecta una amenaza con código malicioso, el módulo antivirus la puede eliminar al bloquearla y luego desinfectarla, eliminándola o enviándola a [Cuarentena](#).

1.4.2 Protección antispam

La protección antispam incorpora múltiples tecnologías (tales como RBL, DNSBL, huellas digitales, verificación de reputación, análisis de contenido, filtro bayesiano, reglas, creación manual de listas blancas y negras, etc.) para maximizar la detección de amenazas provenientes del correo electrónico. El motor de exploración antispam produce un valor de probabilidad en la forma de un porcentaje (0 a 100) para cada mensaje de correo electrónico explorado.

ESET Mail Security también puede utilizar el método de Listas grises (deshabilitado de manera predeterminada) para el filtrado de spam. Este método se basa en la especificación RFC 821, que indica que, como el protocolo SMTP se considera un protocolo de transporte no confiable, cada agente de transferencia de mensajes (MTA) debe intentar enviar reiteradamente un correo electrónico al encontrarse con un error temporal en el envío. Muchos mensajes de spam se entregan de una vez a una lista masiva de direcciones de correo electrónico generada automáticamente. Las listas grises, calculan un valor de control (hash) para la ruta de retorno del remitente, la ruta de retorno del destinatario y la dirección IP del MTA que realiza el envío. Si el servidor no logra encontrar el valor de control para el trío en su base de datos, se rehúsa a recibir el mensaje y devuelve un código de error temporal (por ejemplo, 451). Un servidor legítimo intentará volver a enviar el mensaje tras un lapso variable de tiempo. El valor de control del trío se guardará en la base de datos de conexiones verificadas en el segundo intento, permitiendo que cualquier correo electrónico de características relevantes se distribuya de ese momento en adelante.


1.4.3 Aplicación de reglas definidas por el usuario




La protección basada en reglas definidas está disponible para explorar tanto con VSAPI como con el agente de transporte. Puede utilizar la interfaz del usuario de ESET Mail Security para crear reglas individuales que también se pueden combinar entre sí. Si una regla usa varias condiciones, las condiciones se vincularán usando el operador lógico AND. En consecuencia, la regla se ejecutará únicamente cuando se cumplan todas sus condiciones. Si se crean varias reglas, se aplicará el operador lógico OR, lo que significa que el programa ejecutará la primera regla para la cual se cumplan las condiciones.


En la secuencia de exploración, la primera técnica utilizada es la lista gris, si se encuentra habilitada. Los procedimientos subsiguientes siempre ejecutarán estas técnicas: protección basada en las reglas definidas por el usuario, luego, la exploración antivirus y, finalmente, una exploración antispam.


1.5 Interfaz del usuario


ESET Mail Security posee una interfaz de usuario gráfico (GUI) intuitiva que le brinda a los usuarios un acceso simple a las funciones del programa principales. La ventana principal de ESET Mail Security se encuentra dividida en dos secciones principales. La ventana principal que está a la derecha muestra información correspondiente a la opción seleccionada en el menú principal de la izquierda.


 **MAIL SECURITY**
FOR MICROSOFT EXCHANGE SERVER





 **CONTROL**


 ARCHIVOS DE REGISTRO


 **EXPLORAR**


 CUARENTENA DE CORREO


 ACTUALIZACIÓN


 CONFIGURACIÓN

 HERRAMIENTAS

 AYUDA Y SOPORTE

 **Protección máxima**

 **Licencia**
Válida hasta: 31-Dec-16

 **La base de datos de firmas de virus está actualizada**
última actualización: 25-Aug-15 3:57:02 PM

Estadísticas de la protección del sistema de archivos

Infectados:	0
Desinfectados:	0
No infectados:	41442
Total:	41442

Versión del producto	6.2.10009.1
Nombre del servidor	delta.contoso.lan
Sistema	Windows Server 2012 R2 Standard 64-bit (6.3.9600)
Equipo	Intel(R) Xeon(R) CPU X5660 @ 2.80GHz (2600 MHz), 10240 MB RAM
Tiempo límite del servidor	57 minutos
Total del buzón de correo	6 dominio, 6 local

ENJOY SAFER TECHNOLOGY™

Las diferentes secciones del menú principal se describen a continuación:

- [Supervisión](#): proporciona la información sobre el estado de protección de ESET Mail Security, la validez de la licencia, actualizaciones de la base de datos de firmas de virus, las estadísticas básicas y la información del sistema.
- [Archivos de registro](#): accede a los archivos de registro que contienen información sobre todos los sucesos importantes del programa. Estos archivos proporcionan una visión general de las amenazas detectadas y de otros eventos relacionados con la seguridad.
- [Explorar](#): le permite configurar y ejecutar una Exploración de almacenamiento, una Exploración inteligente, una Exploración personalizada o la Exploración de medios extraíbles. También puede repetir la última exploración que se ejecutó.
- [Cuarentena de correo](#): proporciona una administración sencilla de los correos electrónicos en cuarentena. Este administrador de Cuarentena de correo es común para los tres tipos: cuarentena local, cuarentena de casilla de correo y cuarentena de MS Exchange.
- [Actualización](#): proporciona la información acerca de la base de datos de firmas de virus y le informa acerca de las actualizaciones disponibles. La activación del producto también puede realizarse desde esta sección.
- [Configuración](#): aquí puede ajustar la configuración de seguridad del servidor y del equipo.
- [Herramientas](#): proporciona información adicional acerca de la protección del sistema. Herramientas adicionales que le ayudan a administrar la seguridad. La sección Herramientas contiene los siguientes artículos: [Procesos activos](#), [Observar la actividad](#), [Estadísticas de la protección](#), [Cluster](#), [Shell de ESET](#), [ESET SysInspector](#), [ESET SysRescue Live](#) para crear un CD o USB de recuperación y [Tareas programadas](#). También puede [Enviar el archivo para su análisis](#) y revisar su [Cuarentena](#).
- [Ayuda y soporte](#): brinda acceso a las páginas de ayuda, a la [Base de conocimiento de ESET](#) y a otras herramientas de soporte. También se encuentran disponibles los enlaces para abrir una solicitud de soporte para Atención al cliente y la información acerca de la activación del producto.

Además de la interfaz gráfica principal, hay una **ventana de configuración avanzada**, a la que se puede acceder desde cualquier sección del programa con la tecla F5.

Desde esta ventana de configuración avanzada, se pueden configurar las opciones y preferencias según sus necesidades. El menú de la izquierda incluye en las siguientes categorías: **Servidor**, **Equipo**, **Actualizar**, **Internet y correo electrónico**, **Control del dispositivo**, **Herramientas** e **Interfaz del usuario**. Cuando hace clic en un elemento (categoría o subcategoría) en el menú de la izquierda, se muestra la respectiva configuración del elemento en el panel derecho.

1.6 Requisitos del sistema

Sistemas operativos compatibles:

- Microsoft Windows Server 2003 SP2 (x86 y x64)
- Microsoft Windows Server 2003 R2 (x86 y x64)
- Microsoft Windows Server 2008 (x86 y x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016 (ESET Mail Security 6.4.10011.1)
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

NOTA

la versión compatible mínima de SO es Microsoft Windows Server 2003 SP2.

Versiones compatibles de Microsoft Exchange Server:

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU5, CU6, CU7, CU8, CU9, CU10, CU11, CU12, CU13, CU14
- Microsoft Exchange Server 2016 CU1, CU2, CU3

Los requisitos de hardware dependen de la versión del sistema operativo usada. Se recomienda leer la documentación del producto Microsoft Windows Server y Microsoft Exchange Server para obtener información detallada sobre los requisitos de hardware.

i NOTA

Recomendamos firmemente instalar el último Service Pack de su sistema operativo Microsoft Server y la aplicación del servidor antes de instalar el producto de seguridad de ESET. Además, le recomendamos instalar las últimas actualizaciones y revisiones de Windows cuando estén disponibles.

1.6.1 ESET Mail Security características y roles de Exchange Server

La tabla a continuación le permite identificar qué características están disponibles para cada versión compatible de Microsoft Exchange Server y sus roles. El asistente de instalación de ESET Mail Security comprueba el entorno durante la instalación y una vez instalado, ESET Mail Security mostrará las características según la versión detectada de Exchange Server y sus roles.

	Característica					
	Protección antisпам	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos a petición	Protección de la base de datos del buzón de correo electrónico	Cuarentena de correo
Exchange Server 2003 (instalación del servidor único con roles múltiples)	✓	✓	✓	✗	✓	✓
Exchange Server 2003 (Servidor Front-end)	✓	✓	✓	✗	✗	✓
Exchange Server 2003 (Servidor Back-end)	✓	✓	✓	✗	✓	✓
Exchange Server 2007 (instalación del servidor único con roles múltiples)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2007 (Rol del servidor de Transporte Edge)	✓	✓	✓	✗	✗	✓
Microsoft Exchange Server 2007 (Rol del servidor de Transporte Hub)	✓	✓	✓	✓	✗	✓
Microsoft Exchange Server 2007 (Rol del servidor del buzón de correo)	✗	✓	✗	✓	✓	✗
Microsoft Exchange Server 2010	✓	✓	✓	✓	✓	✓

<i>(instalación del servidor único con roles múltiples)</i>						
Microsoft Exchange Server 2010 <i>(Rol del servidor de Transporte Edge)</i>	✓	✓	✓	✗	✗	✓
Microsoft Exchange Server 2010 <i>(Rol del servidor de Transporte Hub)</i>	✓	✓	✓	✓	✗	✓
Microsoft Exchange Server 2010 <i>(Rol del servidor del buzón de correo)</i>	✗	✓	✗	✓	✓	✗
Microsoft Exchange Server 2013 <i>(instalación del servidor único con roles múltiples)</i>	✓	✓	✓	✓	✗	✓
Microsoft Exchange Server 2013 <i>(Rol del servidor de Transporte Edge)</i>	✓	✓	✓	✗	✗	✓
Microsoft Exchange Server 2013 <i>(Rol del servidor del buzón de correo)</i>	✓	✓	✓	✓	✗	✓
Microsoft Exchange Server 2016 <i>(Rol del servidor de Transporte Edge)</i>	✓	✓	✓	✗	✗	✓
Microsoft Exchange Server 2016 <i>(Rol del servidor del buzón de correo)</i>	✓	✓	✓	✓	✗	✓
Windows Small Business Server 2003	✓	✓	✓	✗	✓	✓
Windows Small Business Server 2008	✓	✓	✓	✓	✓	✓
Windows Small Business Server 2011	✓	✓	✓	✓	✓	✓

1.6.1.1 Roles de Exchange Server: comparación de Edge y Hub

Tanto los servidores Transporte Edge como Transporte Hub tienen las características antispam deshabilitadas de manera predeterminada. Esta es la configuración deseada en una organización de Exchange con el servidor Transporte Edge. Recomendamos que el servidor Transporte Edge tenga activado el antispam ESET Mail Security configurado para filtrar los mensajes antes de que se distribuyan a la organización Exchange.

El rol de Edge es la ubicación preferida para la exploración antispam ya que permite a ESET Mail Security rechazar el spam durante la primera etapa del proceso sin sobrecargar innecesariamente los niveles de red. Con esta configuración, ESET Mail Security filtra los mensajes entrantes en el servidor Transporte Edge, para que puedan moverse con seguridad al servidor Transporte Hub sin necesidad de un filtro adicional.

Si su organización no utiliza el servidor Transporte Edge y solo cuenta con el servidor Transporte Hub, se recomienda habilitar las características antispam en el servidor Transporte Hub que reciba mensajes entrantes desde Internet a través de SMTP.

1.6.1.2 Roles de Exchange Server 2013

La arquitectura de Exchange Server 2013 es diferente a versiones anteriores de Microsoft Exchange. Desde la presentación de 2013, CU4 (que en realidad es el SP1 para Exchange 2013) ha reintroducido el rol del servidor Transporte Edge.

Si está planeando proteger Microsoft Exchange 2013 con ESET Mail Security, asegúrese de instalarlo ESET Mail Security en un sistema que ejecute Microsoft Exchange 2013 con el servidor de la Casilla de correo o el rol del servidor Transporte Edge.

Existe una excepción si planea instalar ESET Mail Security en Windows SBS (Small Business Server) o si tiene Microsoft Exchange 2013 con roles múltiples en un servidor único. En este caso, todos los roles de Exchange se ejecutan en el mismo servidor, por lo cual ESET Mail Security ofrecerá una protección completa, incluida la protección de los servidores de correo.

Si instala ESET Mail Security en un sistema que ejecuta únicamente el rol del servidor de Acceso del cliente (servidor dedicado CAS), las características más importantes de ESET Mail Security se deshabilitarán, en especial las características del servidor de correo. En este caso, solo funcionarán la protección del sistema de archivos en tiempo real y algunos componentes que pertenecen a la [Protección del equipo](#), por lo cual los servidores de correo no estarán protegidos. Por este motivo, no recomendamos instalar ESET Mail Security en un servidor que tenga el rol de servidor de Acceso del cliente. Esto no se aplica a Windows SBS (Small Business Server) y Microsoft Exchange con roles múltiples en el mismo equipo como se mencionó anteriormente.

i NOTA

Debido a las restricciones técnicas de Microsoft Exchange 2013, ESET Mail Security no es compatible con el rol del servidor de Acceso del cliente (CAS). Esto no se aplica a Windows SBS o Microsoft Exchange 2013 instalados en un servidor único con todos los roles del servidor, en este caso, puede ejecutar ESET Mail Security con el rol de CAS en el servidor, ya que el servidor del Buzón de correo y el servidor Transporte Edge estarán protegidos.

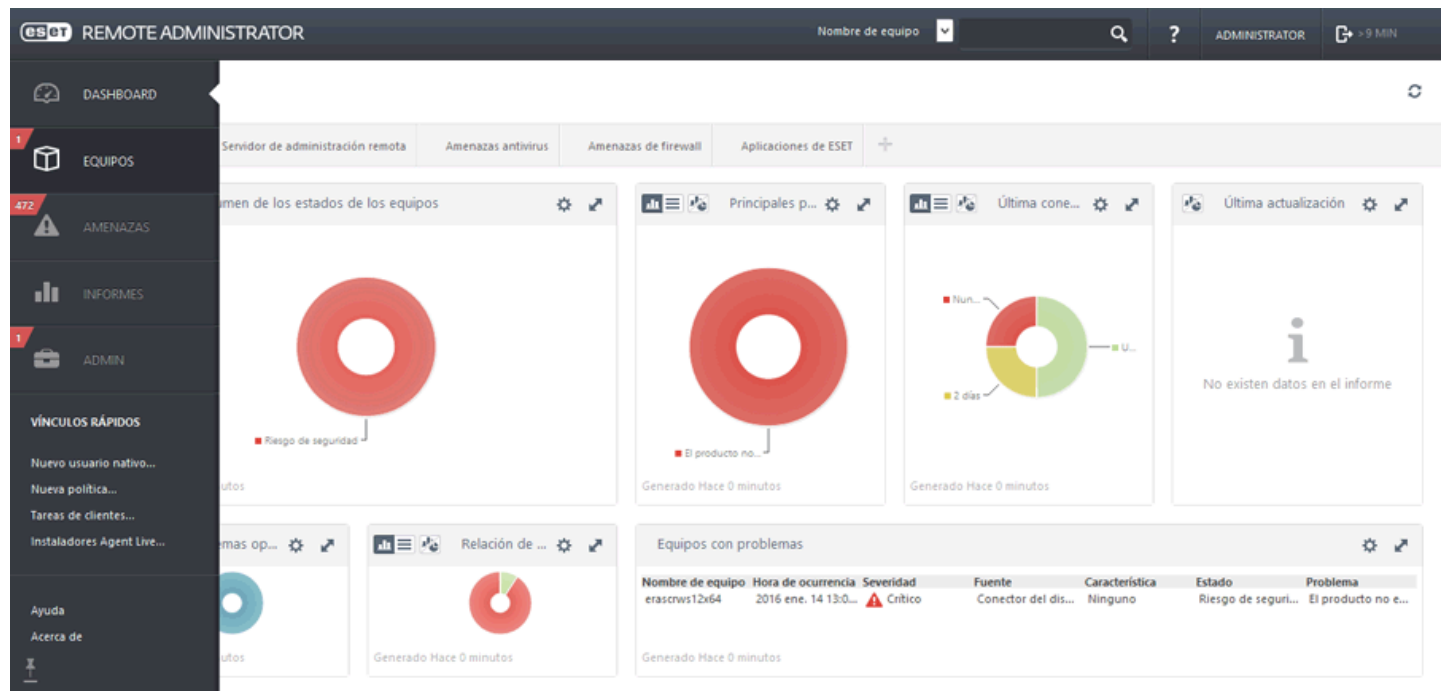
1.7 Administrado a través de ESET Remote Administrator

ESET Remote Administrator (ERA) es una aplicación que le permite administrar los productos ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas ESET Remote Administrator le permite instalar soluciones de seguridad ESET en equipos remotos y responder rápidamente a nuevos problemas y amenazas. ESET Remote Administrator no brinda protección contra códigos maliciosos por sí mismo, sino que confía en la presencia de las soluciones de seguridad ESET en cada cliente.

Las soluciones de seguridad ESET son compatibles con redes que incluyen varios tipos de plataformas. Su red puede incluir una combinación de los sistemas operativos actuales de Microsoft, basados en Linux y Mac, y los sistemas operativos que operen en los dispositivos móviles (teléfonos móviles y tabletas).

- [Servidor de ESET Remote Administrator](#): el servidor ERA se puede instalar en Windows, además de los servidores Linux, y también se presenta como Aparato virtual. Maneja la comunicación con los agentes y recopila y archiva datos de la aplicación.
- La [Consola web ERA](#) es una interfaz del usuario basada en la web que presenta la información del servidor ERA y le permite administrar las soluciones de seguridad ESET en su entorno. Se puede acceder a la consola web a través de un [navegador web](#). Muestra una visión general del estado de los clientes en su red y se puede usar para implementar las soluciones de ESET en equipos no administrados de manera remota. Si decide que el servidor web sea accesible desde Internet, puede usar ESET Remote Administrator desde prácticamente cualquier dispositivo con una conexión a Internet activa.

- **Agente ERA:** el agente ESET Remote Administrator facilita la comunicación entre el Servidor ERA y los equipos cliente. Debe instalar el agente en todos los equipos cliente para establecer una comunicación entre ellos y el Servidor ERA. Dado que se ubica en el equipo cliente y puede almacenar diferentes escenarios de seguridad, el uso del agente ERA disminuye significativamente el tiempo de reacción frente a amenazas nuevas. A través de la consola web, puede [implementar el agente ERA](#) en equipos sin gestión y reconocidos por medio de su Active Directory o por ESET Rogue Detection Sensor.



NOTA

Para obtener más información acerca de ERA, consulte la Ayuda en línea de ESET Remote Administrator. La Ayuda en línea se divide en tres partes: [Instalación/actualización](#), [Administración](#) e [Implementación de aplicación virtual](#). Puede usar las pestañas de navegación superior que se encuentran en el encabezado para alternar entre las partes.

2. Instalación

Luego de adquirir ESET Mail Security, el programa de instalación puede descargarse desde el sitio web de ESET (www.eset-la.com) como un paquete .msi.

Tenga en cuenta que tiene que ejecutar el programa de instalación con la cuenta Administrador incorporado o una cuenta de administrador de dominio (en caso de que tenga la cuenta Administrador incorporado deshabilitada). Cualquier otro usuario, sin importar si es miembro del grupo de Administradores, no tendrá los derechos de acceso suficientes. Por ello, necesita usar una cuenta Administrador incorporado, ya que no podrá completar la instalación exitosamente con otra cuenta de usuario que no sea la de un administrador local o de dominio.

Hay dos modos de ejecutar el programa de instalación:

- Puede iniciar sesión localmente con las credenciales de cuenta del Administrador y sólo ejecutar el programa de instalación
- Puede iniciar sesión como otro usuario, pero debe abrir el símbolo de comandos con Ejecutar como... y escribir las credenciales de cuenta del Administrador para que el comando se ejecute como Administrador; luego escriba en el comando para ejecutar el programa de instalación (por ejemplo `msiexec /i emsx_nt64_ENU.msi` pero debe reemplazar `emsx_nt64_ENU.msi` con el nombre de archivo exacto del programa de instalación msi que descargó)

Una vez abierto el instalador y aceptado el Contrato de licencia de usuario final (EULA, por sus siglas en inglés), el asistente de instalación lo guiará durante la configuración inicial. Si desea no aceptar los términos en el Contrato de licencia, el asistente finalizará.

Completa

Este es el tipo de instalación recomendado. Instala todas las características de ESET Mail Security. Luego de seleccionar el tipo de instalación, deberá especificar las carpetas donde instalar el producto, aunque puede aceptar las carpetas de instalación predefinidas por defecto (recomendado). El instalador instala todas las características del programa en forma automática.

Personalizada

La instalación personalizada le permite seleccionar qué características de ESET Mail Security instalar en su sistema. Verá un listado estándar de características/componentes entre los que elegir para la instalación.

Además de poder usar el asistente de instalación, puede elegir instalar ESET Mail Security en forma silenciosa a través de una línea de comando. Este tipo de instalación no necesita interacción alguna, como cuando se usa el asistente. Es útil para automatizaciones o simplificación. Este tipo de instalación también se llama sin supervisión, dado que no le pide al usuario que interactúe.

Instalación silenciosa/sin supervisión

Completar la instalación a través de la línea de comando: `msiexec /i <packagename> /qn /l*xv msi.log`

IMPORTANTE

se recomienda firmemente instalar ESET Mail Security en un sistema operativo recién instalado y configurado, de ser posible. Sin embargo, si necesita instalarlo en un sistema existente, la mejor forma de hacerlo es desinstalar la versión anterior de ESET Mail Security, reiniciar el servidor y luego instalar la versión nueva ESET Mail Security.

NOTA

si ya ha usado anteriormente otro software de antivirus de terceros en su sistema, le recomendamos que lo desinstale completamente antes de la instalación de ESET Mail Security. Para hacerlo, puede usar [ESET AV Remover](#), que facilita la desinstalación.

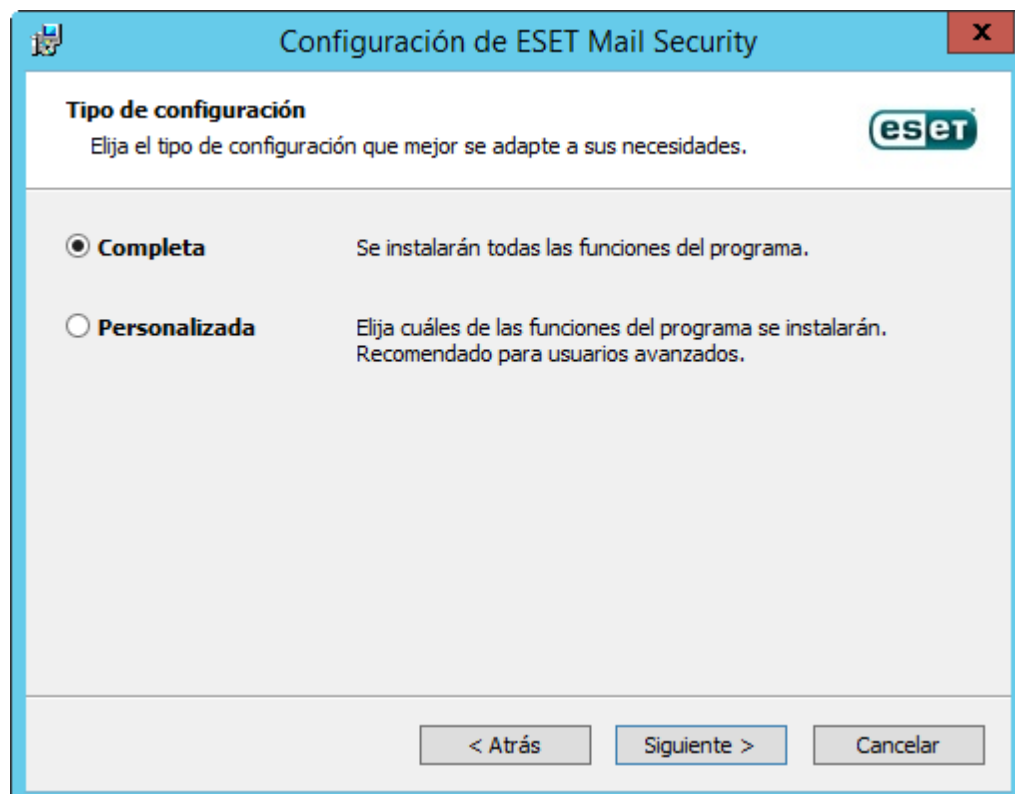
2.1 ESET Mail Security pasos de instalación

Siga los siguientes pasos para instalar ESET Mail Security con el Asistente de configuración:



Después de aceptar el EULA, seleccione uno de los siguientes tipos de instalación:

- **Completa:** instala todas las características de ESET Mail Security. Este es el tipo de instalación recomendada.
- **Personalizada:** selecciona las características de ESET Mail Security que se instalarán en su sistema.



Instalación completa:

también llamada instalación integral. Esto instalará todos los componentes de ESET Mail Security. Se le solicitará

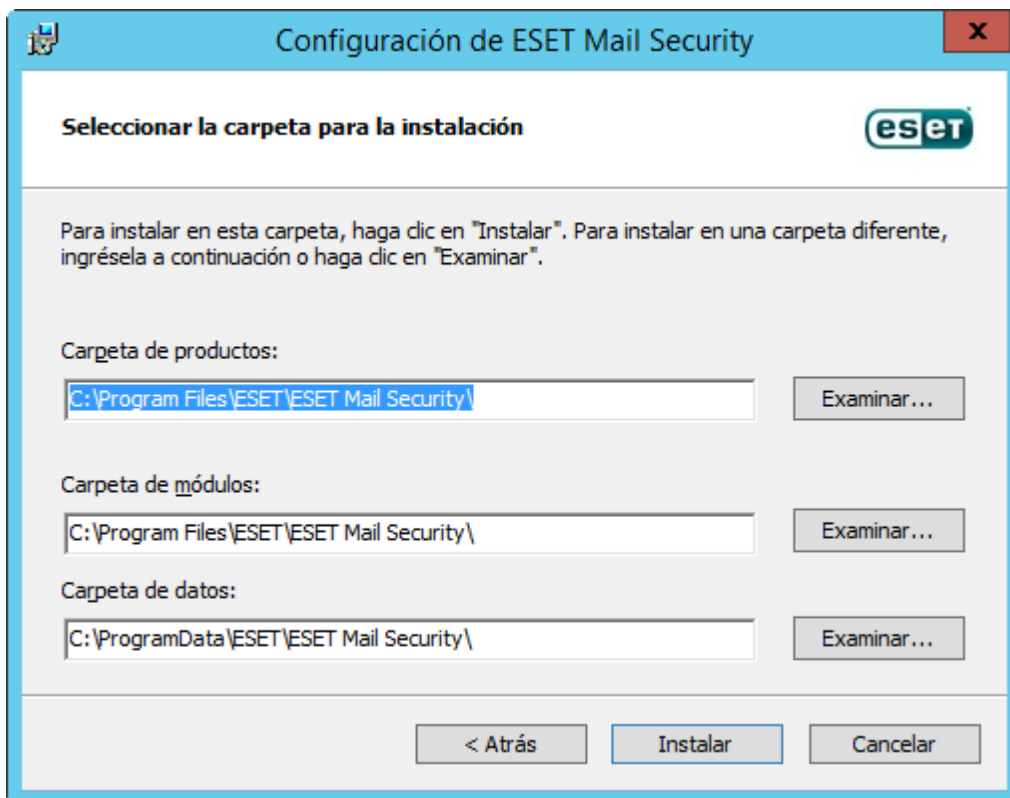
que seleccione la ubicación en la cual se instalará ESET Mail Security. En forma predeterminada, el programa se instala en C:\Archivos de programa\ESET\ESET Mail Security. Haga clic en **Examinar** para cambiar esta ubicación (no recomendado).

i NOTA

En Windows Server 2008 y Windows Server 2008 R2, la instalación del componente **Internet y correo electrónico** está desactivada de manera predeterminada. Si desea instalar este componente, seleccione el tipo de instalación **Personalizada**.

i NOTA

En caso de que planea utilizar [cuarentena local](#) para los mensajes de correo electrónico y no desea que los archivos de mensaje en cuarentena se almacenen en su unidad c:, cambie la ruta de la **carpeta de datos** con su unidad y ubicación preferidas. Sin embargo, tenga en cuenta que todos los archivos de datos de ESET Mail Security se almacenarán en esta ubicación.



Instalación personalizada:

Le deja seleccionar qué características instalar. Útil cuando se quiere personalizar ESET Mail Security solamente con los componentes que necesita.



Puede agregar o quitar componentes incluidos en su instalación. Para hacerlo, ejecute el paquete de instalador *.msi* que usó durante la instalación inicial, o vaya a **Programas y características** (accesible desde el Panel de control de Windows), haga clic con el botón secundario en ESET Mail Security y seleccione **Cambiar**. Siga los siguientes pasos para agregar o quitar componentes.

Proceso de modificación de componentes (agregar/eliminar), reparar y eliminar:

Hay tres opciones disponibles. Puede **Modificar** los componentes instalados, **Reparar** la instalación de ESET Mail Security o **Eliminar** (desinstalar) por completo.



Si selecciona **Modificar** se muestra un listado de los componentes de programa disponibles. Seleccione los componentes que desea agregar o quitar. Puede agregar/eliminar varios componentes al mismo tiempo. Haga clic en el componente y seleccione una opción desde el menú desplegable:



Cuando haya seleccionado una opción, haga clic en **Modificar** para realizar las modificaciones.

i NOTA

puede modificar los componentes instalados en cualquier momento al ejecutar el instalador. En el caso de la mayor parte de los componentes, no es necesario reiniciar el servidor para realizar el cambio. La GUI se reiniciará y solo verá los componentes que eligió tener instalados. En el caso de los componentes que exijan un reinicio del servidor, el Instalador de Windows le solicitará que reinicie y los nuevos componentes estarán disponibles una vez que el servidor esté en línea nuevamente.

2.1.1 Instalación de la línea de comandos

Se espera que se usen las siguientes configuraciones **solo con los niveles reducido, básico y ninguno** de la interfaz del usuario. Consulte la [documentación](#) para obtener la versión **msiexec** usada para los modificadores de la línea de comandos correspondientes.

Parámetros admitidos:

APPDIR=<path>

- ruta - Ruta de directorio válida
- Directorio de instalación de aplicación.
- Por ejemplo: `emsx_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- ruta - Ruta de directorio válida
- Directorio de instalación de los datos de la aplicación.

MODULEDIR=<path>

- ruta - Ruta de directorio válida
- Directorio de instalación del módulo.

ADDEXCLUDE=<list>

- La lista ADDEXCLUDE es una lista separada por comas de los nombres de las características que no se van instalar, como un reemplazo del obsoleto QUITAR.
- Cuando se selecciona no instalar una característica, entonces toda la ruta (es decir, todas las subcaracterísticas) y las características invisibles relacionadas deben incluirse explícitamente en la lista.
- Por ejemplo: `ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network`

i NOTA

los **ADDEXCLUDE** no se puede usar junto con **ADDLOCAL**.

ADDLOCAL=<list>

- Instalación de componente: lista de características no obligatorias que se instalarán en forma local.
- Se usa con los paquetes de ESET .msi: `emsx_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para más información sobre la propiedad **ADDLOCAL**, consulte <http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>

Reglas

- El **ADDLOCAL list** es una lista separada por comas de todos los nombres de las características que se instalarán.
- Al seleccionar una característica para instalar, toda la ruta (todas las características principales) deberá incluirse de forma explícita en la lista.
- Vea reglas adicionales para usarlo correctamente.

Presencia de característica

- **Obligatoria:** la característica se instalará siempre
- **Opcional:** se podrá deseleccionar la característica durante la instalación
- **Invisible:** función lógica obligatorio para que otras características funcionen correctamente
- **Marcador:** característica que no tiene ningún efecto en el producto, pero debe figurar con las sub-funciones

El árbol de características es el siguiente:

Árbol de características	Nombre de característica	Presencia de característica
Equipo	Equipo	Obligatoria
Equipo / Antivirus y antispyware	Antivirus	Obligatoria
Equipo / Antivirus y antispyware > Protección del sistema de archivos en tiempo real	Protección en tiempo real	Obligatoria
Equipo / Antivirus y antispyware > Exploración del equipo	Exploración	Obligatoria
Equipo / Antivirus y antispyware > Protección de documentos	Protección de documentos	Opcional
Equipo / Control del dispositivo	Control de dispositivos	Opcional
Red	Red	Marcador
Red / Firewall personal	Firewall	Opcional
Internet y correo electrónico	Internet y correo electrónico	Marcador
Filtrado de protocolo Web y de correo electrónico	Filtrado de protocolos	Invisible
Web y correo electrónico / Protección del acceso a la Web	Protección del acceso a la Web	Opcional
Web y correo electrónico / Protección de cliente de correo electrónico	Protección del cliente de correo electrónico	Opcional
Web y correo electrónico / Protección de cliente de correo electrónico / Complementos de correo	Complementos de correo	Invisible
Web y correo electrónico / Protección de cliente de correo electrónico / Protección antispam	Antispam	Opcional
Web y correo electrónico / Control Web	Control Web	Opcional
Mirror de actualización	Mirror de actualización	Opcional
Soporte de Microsoft NAP	MicrosoftNAP	Opcional

Reglas adicionales

- Si se selecciona una de las características de **Web y correo electrónico** para su desinstalación, la característica invisible **Filtrado de protocolo** debe incluirse explícitamente en la lista.
- Si se selecciona una de las subcaracterísticas de **Protección de cliente de correo electrónico** para su desinstalación, la característica invisible **Complementos de correo** debe incluirse explícitamente en la lista

Ejemplos:

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Listado de CFG_properties:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0

- 0: Deshabilitado, 1: Habilitado

CFG_LIVEGRID_ENABLED=1/0

- 0: Deshabilitado, 1: Habilitado
- LiveGrid

FIRSTSCAN_ENABLE=1/0

- 0: Deshabilitar, 1: Habilitar
- Programar un FirstScan nuevo después de la instalación.

CFG_EPFW_MODE=0/1/2/3

- 0: Automático, 1: Interactivo, 2: Política, 3: Aprendizaje

CFG_PROXY_ENABLED=0/1

- 0: Deshabilitado, 1: Habilitado

CFG_PROXY_ADDRESS=<ip>

- Dirección IP de proxy.

CFG_PROXY_PORT=<port>

- Número de puerto de proxy.

CFG_PROXY_USERNAME="<user>"

- Nombre de usuario para la autenticación.

CFG_PROXY_PASSWORD="<pass>"


- Contraseña para la autenticación.

2.1.2 Instalación en un entorno de clúster

Puede implementar ESET Mail Security en un entorno de clúster (por ejemplo un clúster de conmutación por error). Le recomendamos instalar ESET Mail Security en un nodo activo y luego redistribuir la instalación en nodos pasivos usando la función [Cluster de ESET](#) de ESET Mail Security. Además de la instalación, el clúster de ESET actuará como replicación de la configuración de ESET Mail Security para garantizar la consistencia entre los nodos de clúster necesarios para el funcionamiento correcto.


2.2 Activación del producto

Cuando la instalación se complete, se le solicitará que active el producto.

Activación del producto 

Activar con clave de licencia

- - - -





Su clave de licencia usará el formato
XXXX-XXXX-XXXX-XXXX-XXXX


[¿Dónde puedo encontrar la clave de la licencia?](#)
Ya tengo nombre de usuario y contraseña, ¿cuál es el siguiente paso?

Activar

Otras opciones de activación

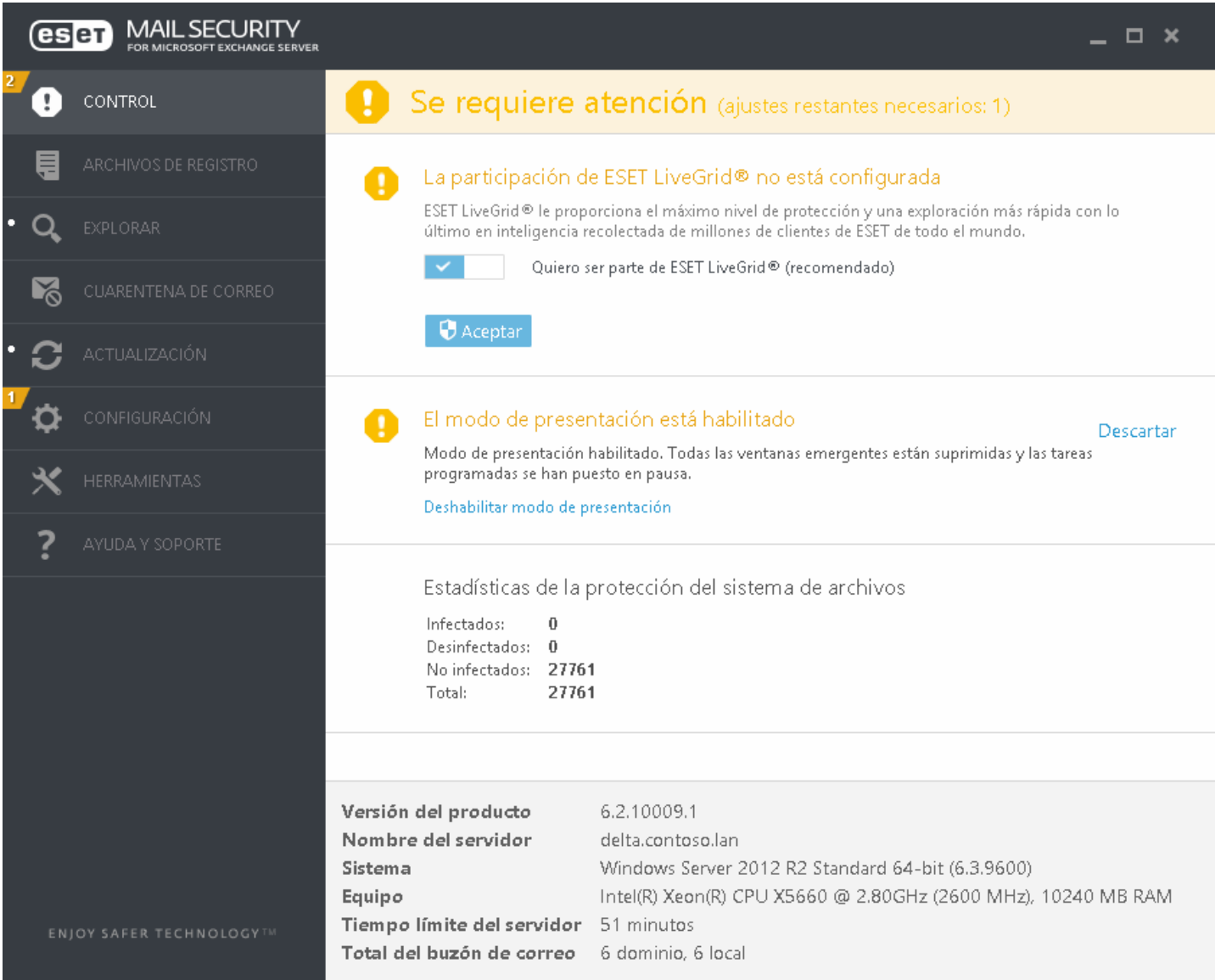
[Security Admin](#)
Activar con una licencia de una cuenta de admin de seguridad.

[Licencia sin conexión](#)
Utilice un archivo de licencia sin conexión si este cliente no se conecta a la red.

[Activar luego](#)
Utilizar ESET Remote Administrator para activar este cliente más tarde.

Seleccione uno de los métodos disponibles para activar ESET Mail Security. Consulte [Cómo activar ESET Mail Security](#) para obtener más información.

Luego de que haya activado ESET Mail Security con éxito, se abrirá la ventana principal del programa y mostrará su estado actual en la página [Supervisión](#). Deberá prestar atención al principio; por ejemplo, se le preguntará si desea ser parte de <%ELG%>.



La ventana principal del programa también mostrará notificaciones sobre otros elementos, como actualizaciones del sistema (Actualizaciones de Windows) o actualizaciones de la base de datos de firmas de virus. Cuando se resuelven todos los elementos que requieren atención, el estado de supervisión se pondrá en color verde y mostrará el estado **Protección máxima**.

2.3 Terminal Server

Si instala ESET Mail Security en un servidor Windows que funciona como Terminal Server, es posible que quiera deshabilitar la interfaz gráfica del usuario de ESET Mail Security para evitar que se inicie cada vez que se registre un usuario. Para ver los pasos específicos para deshabilitarla, consulte el capítulo [Deshabilitación de la interfaz gráfica del usuario en Terminal Server](#).

2.4 ESET AV Remover

Para eliminar o desinstalar el software antivirus de terceros de su sistema, le recomendamos usar la herramienta ESET AV Remover. Para hacerlo, siga estos pasos:

1. Descargue ESET AV Remover desde el sitio web de ESET [Página de descarga de utilidades](#).
2. Haga clic en **Acepto, iniciar la búsqueda** para aceptar el EULA y comenzar a buscar en su sistema.
3. Haga clic en **Iniciar desinstalador** para quitar el software de antivirus instalado.

Para ver una lista de software antivirus de terceros que se pueden eliminar con la herramienta ESET AV Remover, consulte este [artículo de KB](#).

2.5 Conector y antispam POP3

Las versiones de Microsoft Windows Small Business Server (SBS) contienen un conector nativo POP3 incorporado que le permite al servidor obtener mensajes de correos electrónicos desde servidores POP3 externos. La implementación de este conector nativo POP3 de Microsoft difiere entre una versión de SBS y otra.

ESET Mail Security es compatible con el conector POP3 de Microsoft SBS, siempre que se encuentre configurado correctamente. Los mensajes descargados mediante el conector POP3 de Microsoft son escaneados en busca de spam. La protección antispam de estos mensajes es posible ya que el conector POP3 reenvía los mensajes de correo electrónico desde una cuenta POP3 al servidor de Microsoft Exchange mediante SMTP.

ESET Mail Security ha sido evaluado con servicios de correo populares como **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** y **gmx.de** en los siguientes sistemas de SBS:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

! IMPORTANTE

Si utiliza el conector POP3 de Microsoft SBS incorporado y todos los mensajes son escaneados en busca de spam, diríjase a Configuración avanzada, navegue hasta **Servidor > Protección del transporte de correo > Configuración avanzada** y en la configuración **Explorar también los mensajes procedentes de conexiones autenticadas o internas** seleccione **Explorar con la protección antispam y antivirus** de la lista desplegable. Esto asegura la protección antispam para los correos obtenidos desde cuentas POP3.

También puede utilizar un conector POP3 de terceros como P3SS (en lugar del conector POP3 incorporado de Microsoft SBS). ESET Mail Security ha sido evaluado en los siguientes sistemas (utilizando el conector P3SS para obtener mensajes de **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** y **gmx.de**):

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 con Exchange Server 2007
- Microsoft Windows Server 2008 R2 con Exchange Server 2010
- Microsoft Windows Server 2012 R2 con Exchange Server 2013

2.6 Reemplazo por una versión más nueva

Las versiones nuevas de ESET Mail Security se emiten para brindar mejoras del programa o para resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa. Es posible realizar una actualización desde una versión más antigua de ESET Mail Security (4.5 y anterior) aunque es una actualización a una arquitectura diferente.

- [En forma manual](#), mediante la descarga e instalación de la versión más reciente sobre su versión existente. Simplemente ejecute el instalador y realice la instalación como siempre, ESET Mail Security transferirá su configuración existente automáticamente. Le recomendamos este procedimiento si tiene un único servidor en ejecución ESET Mail Security. Aplicable para las actualizaciones desde cualquier versión anterior a 6.x.
- [En forma remota](#), en un entorno de red grande mediante ESET Remote Administrator. Este método es útil si tiene varios servidores en ejecución ESET Mail Security. Aplicable para las actualizaciones desde la versión 4.x a 6.x.
- Puede usar el [Asistente de clúster de ESET](#) como método de actualización. Es un procedimiento muy simple que le permite actualizar las versiones anteriores de ESET Mail Security que se ejecutan en sus servidores. Además, una vez finalizada la actualización, puede continuar usando el [clúster de ESET](#) y aprovechar las funciones. Recomendamos usar este método para 2 o más servidores con ESET Mail Security. Aplicable para las actualizaciones desde la versión 4.x a 6.x.

NOTA

Será necesario reiniciar el servidor durante la actualización de ESET Mail Security.

IMPORTANTE

Existen algunas excepciones durante la actualización, no se conservarán todas las configuraciones, en particular las Reglas. Esto se debe a la funcionalidad de las Reglas que se diseñaron nueva y completamente en ESET Mail Security 6. Las reglas en las versiones anteriores de ESET Mail Security no son compatibles con las Reglas en la versión 6 de ESET Mail Security. Recomendamos que configure las [Reglas](#) manualmente definiendo las condiciones del filtrado del correo electrónico y las acciones a tomar con el correo electrónico filtrado. Nuevas reglas le dan flexibilidad y aún más posibilidades comparadas con las Reglas en versiones anteriores de ESET Mail Security.

A continuación encontrará una lista de configuraciones que se conservan de las versiones anteriores de ESET Mail Security:

- Configuración general de ESET Mail Security.
- Configuración de la protección antispam:
 - Todas las configuraciones que sean idénticas en las versiones anteriores, las configuraciones nuevas utilizarán los valores predeterminados.
 - Listas blancas y negras.

NOTA

Una vez que haya actualizado ESET Mail Security, le recomendamos revisar todas las configuraciones para asegurarse de que estén correctamente configuradas y según sus necesidades.

2.6.1 Actualización mediante ERA

[ESET Remote Administrator](#) le permite actualizar varios servidores que ejecutan una versión anterior de ESET Mail Security. Este método tiene la ventaja de actualizar una gran cantidad de servidores a la vez y, al mismo tiempo, se asegura de que cada ESET Mail Security se configure de manera idéntica (si lo desea).

i NOTA

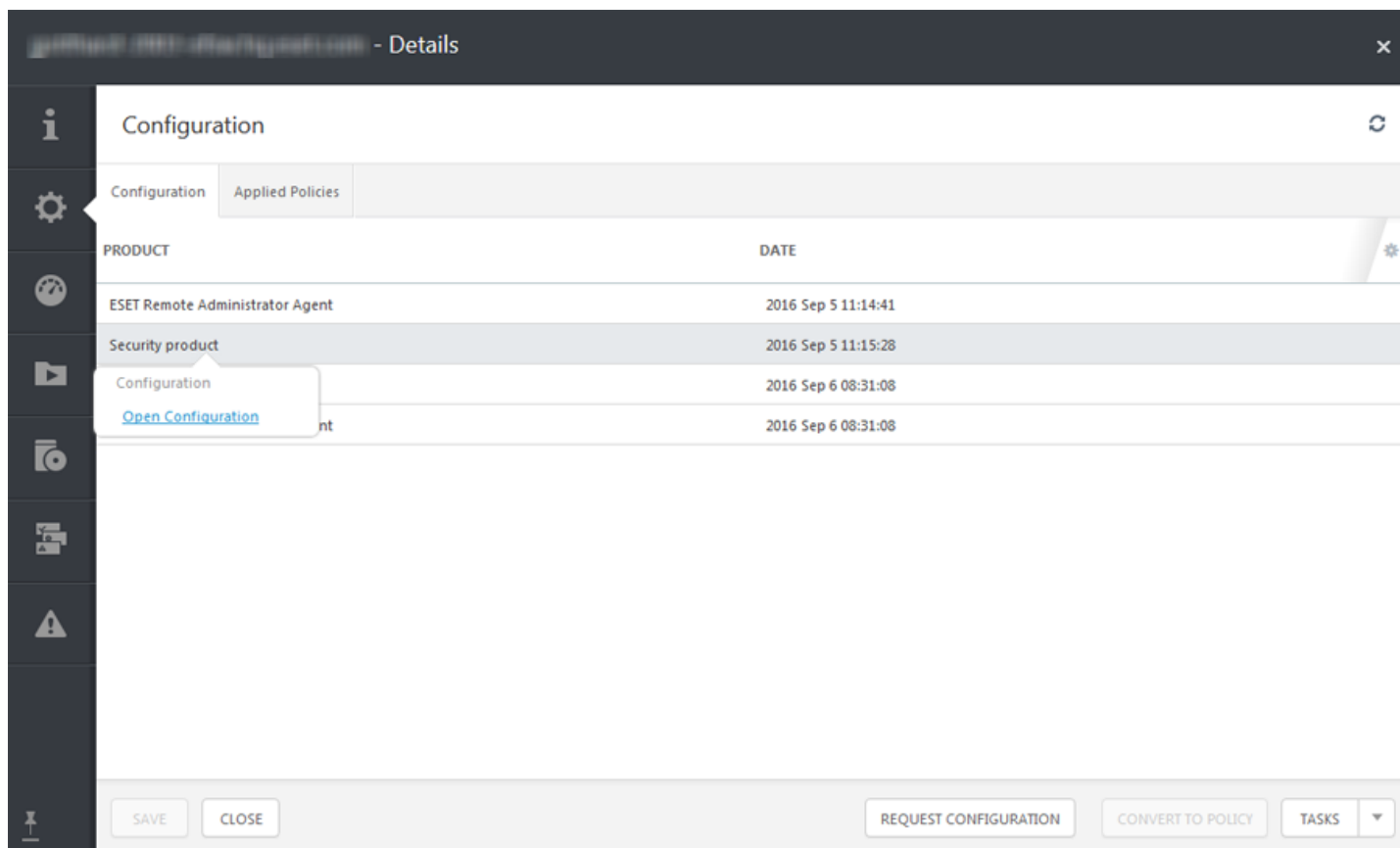
Aplicable para las actualizaciones desde la versión 4.x a 6.x.

El procedimiento consta de las siguientes fases:

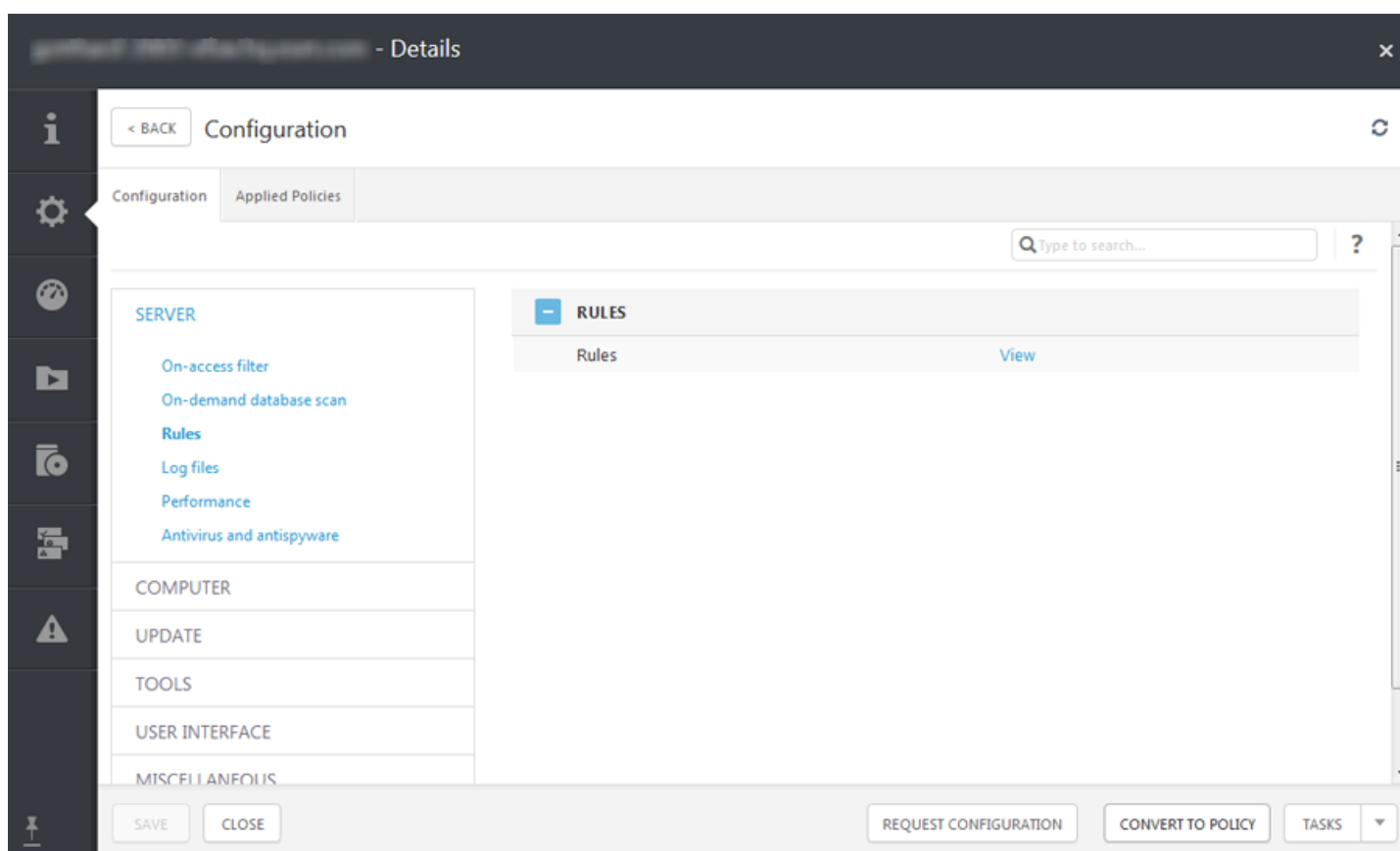
- **Actualice el primer servidor** manualmente mediante la instalación de la versión más reciente de ESET Mail Security sobre su versión existente para preservar toda la configuración, incluso las reglas, las diversas listas blancas y listas negras, etc. Esta fase se realiza a nivel local en el servidor que ejecuta ESET Mail Security.
- **Solicite la configuración** del ESET Mail Security recientemente configurado a la versión 6.x y **Convierta a la política** en ERA. La política se aplicará posteriormente a todos los servidores actualizados. Esta fase se realiza a nivel remoto mediante ERA al igual que las fases siguientes.
- **Ejecute la tarea de desinstalación de software** en todos los servidores que ejecutan la versión anterior de ESET Mail Security.
- **Ejecute la tarea de instalación de software** en todos los servidores en donde desea ejecutar la versión más reciente de ESET Mail Security.
- **Asigne la política de configuración** a todos los servidores que ejecutan la versión más reciente de ESET Mail Security.

Procedimiento paso a paso:

1. Inicie sesión en uno de los servidores que ejecuta ESET Mail Security y actualícelo mediante la descarga e instalación de la última versión respecto de la existente. Siga los [pasos de instalación regular](#). La configuración original de su ESET Mail Security anterior se preservará durante la instalación.
2. Abra la **Consola Web de ERA**, elija un equipo del cliente dentro de los grupos estáticos o dinámicos; para ello, haga clic y seleccione **Detalles**.
3. Navegue en la pestaña [Configuración](#) y haga clic en el botón **Solicitar configuración** para recopilar la configuración del producto gestionado. Llevará un momento obtener la configuración. Cuando aparezca en la lista la configuración más reciente, haga clic en **Producto de seguridad** y elija **Configuración abierta**.



4. Para crear la política de configuración, haga clic en el botón **Convertir a política**. Ingrese el **Nombre** de una nueva política y haga clic en **Finalizar**.



5. Navegue a **Admin > Tareas de clientes** y elija la tarea [Desinstalación de software](#). Al crear la tarea de desinstalación, le recomendamos reiniciar el servidor después de la desinstalación; para ello, seleccione la casilla de verificación **Reiniciar automáticamente cuando fuera necesario**. Después de crear la tarea, agregue los equipos de destino que desee desinstalar.

6. Asegúrese de que ESET Mail Security se desinstale de todos los destinos.
7. Cree la tarea [Instalación de software](#) para instalar la versión más reciente de ESET Mail Security en todos los destinos deseados.
8. **Asigne la política de configuración** a todos los servidores que ejecutan la versión más reciente de ESET Mail Security, idealmente en un grupo.

2.6.2 Actualización mediante el clúster de ESET

La creación del [clúster de ESET](#) le permite actualizar varios servidores con una versión anterior de ESET Mail Security. Es una alternativa a la [actualización mediante ERA](#). Le recomendamos usarla si tiene 2 o más servidores con ESET Mail Security en su entorno. Otro beneficio de este método de actualización es que puede continuar usando el [clúster de ESET](#) para que la configuración de ESET Mail Security esté sincronizada en todos los nodos de los miembros.

NOTA

Aplicable para las actualizaciones desde la versión 4.x a 6.x.

El procedimiento consta de los siguientes pasos:

1. Inicie sesión en uno de los servidores que ejecuta ESET Mail Security y actualícelo mediante la descarga e instalación de la última versión respecto de la existente. Siga los [pasos de instalación regular](#). La configuración original de su ESET Mail Security anterior se preservará durante la instalación.
2. Ejecute el [asistente del clúster de ESET](#) y agregue los nodos del clúster (servidores en los que quiere actualizar ESET Mail Security). Si fuera necesario, puede agregar otros servidores que aún no ejecutan ESET Mail Security (en este caso, se realizará una instalación). Le recomendamos dejar la configuración predeterminada al especificar el [nombre del clúster y el tipo de instalación](#) (asegúrese de tener marcada la opción **Enviar licencia a nodos sin un producto activado**).
3. Revise la pantalla **Registro de verificación de nodos**. Enumerará los servidores que contienen una versión anterior e indicará que se reinstalará el producto. Además, si ha agregado servidores sin ESET Mail Security, tendrán productos instalados:

Node check log

Check

[13:39:36] Node check started
[13:39:36] PING test:
[13:39:36] OK
[13:39:36] Administration share access test:
[13:39:36] OK
[13:39:39] Service manager access test:
[13:39:39] OK
[13:39:39] Checking installed product version and features:
[13:39:42] -2003-SHAREPOINT_2: Older version of the product detected. Product will be reinstalled.
[13:39:43] -2003-CLEAN: Install will be performed.
[13:39:45] OK
[13:39:45] Warning: The product needs to be reinstalled on some machines before creating the cluster. This may cause those machines to be automatically restarted.

< Previous

Next >

Cancel

4. La pantalla **Instalación de nodos y activación del clúster** mostrará el progreso de la instalación. Cuando se complete correctamente, deberá finalizar con resultados similares a estos:

Product install log

[15:53:58] Generating certificates for cluster nodes...
[15:54:01] All certificates created.
[15:54:01] Copying files to remote machines:
[15:54:05] All files have been copied to remote machines.
[15:54:05] Installing product:
[15:55:00] ESET solutions are installed on all remote machines.
[15:55:00] Enrolling certificates:
[15:55:02] All certificates have been enrolled to remote machines.
[15:55:02] Activating cluster feature:
[15:55:03] Cluster feature has been activated on all machines.
[15:55:03] Pushing license to the nodes:
[15:55:05] License has been successfully pushed to the nodes.
[15:55:05] Synchronizing settings:
[15:55:06] Settings have been synchronized.

Install

< Previous

Finish

Cancel

Si su red o DNS no está configurada correctamente, podrá encontrar un mensaje de error que diga **Error al obtener el token de activación del servidor**. Intente ejecutar nuevamente el [asistente del clúster de ESET](#). Destruirá el clúster y generará uno nuevo (sin reinstalar el producto) y esta vez la activación debe finalizar correctamente. Si el problema persiste, verifique su configuración de DNS y red.

Product install log

[18:06:59] Generating certificates for cluster nodes...
[18:07:01] All certificates created.
[18:07:01] Copying files to remote machines:
[18:07:01] All files have been copied to remote machines.
[18:07:01] Enrolling certificates:
[18:07:03] All certificates have been enrolled to remote machines.
[18:07:03] Activating cluster feature:
[18:07:04] Cluster feature has been activated on all machines.
[18:07:04] Pushing license to the nodes:
[18:07:04] Failed to obtain activation token from the server.
[18:07:04] There were errors pushing license to the nodes.
[18:07:04] Synchronizing settings:
[18:07:05] There were errors synchronizing settings in the cluster.

Install

< Previous

Finish

Cancel

3. Guía para principiantes

Este capítulo brinda una vista general de ESET Mail Security, las partes principales del menú, las funcionalidades y las configuraciones básicas.

3.1 Supervisión

El estado de protección en la sección **Supervisión** le informa acerca del nivel de protección actual de su equipo. Se mostrará un resumen de estado del funcionamiento de los módulos de ESET Mail Security en la ventana principal.

✓ El estado **Protección máxima** en color verde indica que la máxima protección está asegurada. La ventana de estado también muestra enlaces rápidos a funciones de uso frecuente en ESET Mail Security y la información acerca de la última actualización.

Se asigna una marca de verificación verde a los módulos que funcionan adecuadamente. Se asigna un signo de exclamación rojo o una notificación naranja a los módulos que no son completamente funcionales. Se muestra la información adicional sobre el módulo en el sector superior de la ventana. También se muestra la solución sugerida para reparar el módulo. Para cambiar el estado de un módulo individual, haga clic en **Configuración** en el menú principal y luego en el módulo deseado.

MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

1

CONTROL

ARCHIVOS DE REGISTRO

EXPLORAR

CUARENTENA DE CORREO

ACTUALIZACIÓN

1

CONFIGURACIÓN

HERRAMIENTAS

AYUDA Y SOPORTE

ENJOY SAFER TECHNOLOGY™

Alerta de seguridad

Protección antivirus del servidor de correo deshabilitada
Descartar

El usuario deshabilitó la protección antivirus del servidor de correo electrónico. [Habilitar la protección antivirus](#)

Estadísticas de la protección del sistema de archivos

Infectados:	0
Desinfectados:	0
No infectados:	65718
Total:	65718

Versión del producto	6.2.10009.1
Nombre del servidor	delta.contoso.lan
Sistema	Windows Server 2012 R2 Standard 64-bit (6.3.9600)
Equipo	Intel(R) Xeon(R) CPU X5660 @ 2.80GHz (2600 MHz), 10240 MB RAM
Tiempo límite del servidor	1 hora, 4 minutos
Total del buzón de correo	6 dominio, 6 local

El ícono rojo indica que hay problemas críticos: la máxima protección del equipo no está asegurada. Este estado se muestra cuando:

- **Protección antivirus y antispyware deshabilitada:** puede volver a habilitar la protección antivirus y antispyware al hacer clic en **Habilitar protección en tiempo real** en el panel **Estado de protección** o en **Habilitar protección antivirus y antispyware** en el panel **Configuración** de la ventana principal del programa.
- Usted usa una base de datos de firmas de virus obsoleta.
- El producto no está activado.
- **La licencia está vencida:** esto se indica cuando el ícono de estado de protección se muestra en rojo. Una vez que se vence la licencia, el programa no se podrá actualizar. Siga las instrucciones en la ventana de alerta para renovar la licencia.

El ícono naranja indica que su producto ESET requiere atención por un problema que no es crítico. Las razones posibles incluyen:


- **La protección del acceso a la Web está deshabilitada:** puede volver a habilitar la protección del acceso a la Web al hacer clic en la notificación de seguridad y luego en **Habilitar la protección del acceso a la Web**.
- **La licencia se vencerá pronto:** esto se indica mediante un ícono de estado de protección que muestra un signo de exclamación. Una vez que se vence la licencia, el programa no podrá actualizarse y el ícono de estado de protección se pondrá rojo.

Encontrará información del sistema en la parte inferior de la página Supervisión. Esta información incluye:

Para acceder a los archivos de registro, diríjase a la ventana principal del programa y haga clic en **Archivos de registro**. Seleccione el tipo de registro deseado desde el menú desplegable. Se encuentran disponibles los siguientes registros:

- **Amenazas detectadas:** el registro de amenazas ofrece información detallada sobre las infiltraciones detectadas por los módulos de ESET Mail Security. Esto incluye la hora de la detección, el nombre de la infiltración, la ubicación, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración. Haga doble clic en la entrada de cualquier registro para mostrar sus detalles en una ventana separada.
- **Eventos:** todas las acciones importantes que ESET Mail Security lleva a cabo se registran en el registro de eventos. El registro de sucesos contiene información sobre los sucesos y errores que se produjeron en el programa. Se diseñó para ayudar a los administradores de sistemas y a los usuarios a resolver problemas. Con frecuencia, la información aquí incluida puede ayudarlo a encontrar una solución a un problema que ocurra en el programa.
- **Exploración del equipo:** todos los resultados de la exploración se muestran en esta ventana. Cada línea corresponde a un control individual de un equipo. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración respectiva.
- **HIPS:** contiene historiales de las reglas específicas que se marcan para su inclusión en el registro. El protocolo muestra la aplicación que desencadenó la operación, el resultado (si la regla se permitió o prohibió) y el nombre de la regla creada.
- **Sitios Web filtrados:** una lista de sitios web que fueron bloqueados por la [Protección del acceso a la Web](#). En estos registros puede ver la hora, la URL, el usuario y la aplicación que abrió una conexión con el sitio web en particular.
- **Control del dispositivo:** contiene registros de medios o dispositivos extraíbles que se conectaron al equipo. Solo los dispositivos con una Regla de control del dispositivo se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, se creará una entrada del registro para un dispositivo conectado. Aquí también puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).
- **Protección del servidor de correo:** aquí se guardan todos los mensajes que ESET Mail Security detecta como infiltración o spam. Estos registros se aplican a los siguientes tipos de protección: Antispam, Reglas y Antivirus. Al hacer doble clic sobre un elemento, se abrirá una ventana emergente con información Adicional acerca del mensaje de correo electrónico detectado, como la **dirección IP, dominio HELO, ID del mensaje, tipo de exploración** que muestra la capa de protección que se detectó. Además, puede visualizar el resultado de la exploración del antivirus y antispam y los motivos de la detección o si se activó un Regla.
- **Exploración de la base de datos:** contiene la versión de la base de datos de firmas de virus, la fecha, la ubicación explorada, la cantidad de objetos escaneados, la cantidad de amenazas encontradas, la cantidad de aciertos de la regla y el tiempo de compleción.
- **Creación de listas grises:** todos los mensajes que se han evaluado usando el método de creación de listas grises se guardan aquí.

En cada una de las secciones, la información mostrada se puede copiar al portapapeles (teclas de acceso directo Ctrl + C) al seleccionar la entrada y hacer clic en **Copiar**. Las teclas CTRL y SHIFT se pueden usar para seleccionar múltiples entradas.

Haga clic en el ícono del interruptor  **Filtrado** para abrir la ventana **Filtrado de registros** donde puede definir los criterios de filtrado.

Puede hacer que el menú contextual aparezca al hacer clic con el botón secundario en un historial específico. Las siguientes opciones se encuentran disponibles en el menú contextual:

- **Mostrar:** muestra información más detallada acerca del registro seleccionado en una ventana nueva (igual que hacer doble clic).
- **Filtrar registros iguales:** activa la filtración de registros y muestra solamente los registros del mismo tipo que el registro seleccionado.
- **Filtrar...:** al hacer clic en esta opción, la ventana [Filtrar registros](#) le permitirá definir los criterios de filtrado para las entradas de registro específicas.
- **Habilitar filtro:** activa las configuraciones de los filtros. La primera vez que filtre los registros, debe definir los criterios de filtrado. Una vez que los filtros están configurados, permanecerán sin cambios hasta que los edite.
- **Deshabilitar filtro:** desactiva los filtros (al igual que el hacer clic en el interruptor en la parte inferior). Esta opción se encuentra disponible solamente cuando el filtrado se encuentra habilitado.
- **Copiar:** copia la información de los registros seleccionados/resaltados al portapapeles.
- **Copiar todo:** copia la información de todos los registros que aparecen en la ventana.
- **Eliminar:** elimina los registros seleccionados/resaltados. Esta acción requiere contar con privilegios de administrador.
- **Eliminar todo:** elimina todos los registros en la ventana. Esta acción requiere privilegios de administrador.
- **Exportar...:** exporta la información de los registros seleccionados/resaltado a un archivo .xml.
- **Exportar todo...** - Exporta toda la información de la ventana a un archivo .xml.
- **Buscar...:** abre la ventana [Buscar en los registros](#) y le permite definir los criterios de búsqueda. Trabaja sobre el contenido que ya se filtró como medio adicional para reducir los resultados.
- **Buscar siguiente:** busca la siguiente concordancia con la búsqueda definida con anterioridad (ver arriba).
- **Buscar anterior:** busca la concordancia anterior con la búsqueda definida con anterioridad (ver arriba).
- **Eliminar los registros de diagnóstico:** elimina todos los registros en la ventana.
- **Desplazar registro:** deje esta opción habilitada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana **Archivos de registro**.

3.2.1 Registro de exploración

La ventana de registro de exploración muestra el estado actual de la exploración junto con información sobre la cantidad detectada de archivos con códigos malintencionados.

Exploración del equipo

Registro

Registro de la exploración

Versión de la base de datos de firmas de virus: 14255 (20161010)

Fecha: 10/10/2016 Hora: 3:52:31 PM

Discos, carpetas y archivos explorados: Memoria operativa;C:\Sector de inicio;E:\Sector de inicio;C:\E\

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\7cc1b35a02cafe07523e - error al abrir [4]

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\Temp\ZAPDFCF.tmp\System.Configuration.dll - error al a...

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\Temp\ZAP9889.tmp\System.Windows.Forms.dll - error al ...

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\30869a7c1acf3a4617b8 - error al abrir [4]

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\System\c8c33f01cccbd17232e8 - error al abrir [4]

Memoria operativa = C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\5bd3374f05d46ba0563f - error al abrir [4]

C:\Documents and Settings\Administrator\NTUSER.DAT - error al abrir [4]

C:\Documents and Settings\Administrator\ntuser.dat.LOG1 - error al abrir [4]

C:\Documents and Settings\Administrator\ntuser.dat.LOG2 - error al abrir [4]

C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat - error al abrir [4]

C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error al abrir [4]

☐ Filtrado

En cada una de las secciones, la información mostrada se puede copiar al portapapeles (teclas de acceso directo Ctrl + C) al seleccionar la entrada y hacer clic en **Copiar**. Las teclas CTRL y SHIFT se pueden usar para seleccionar múltiples entradas.

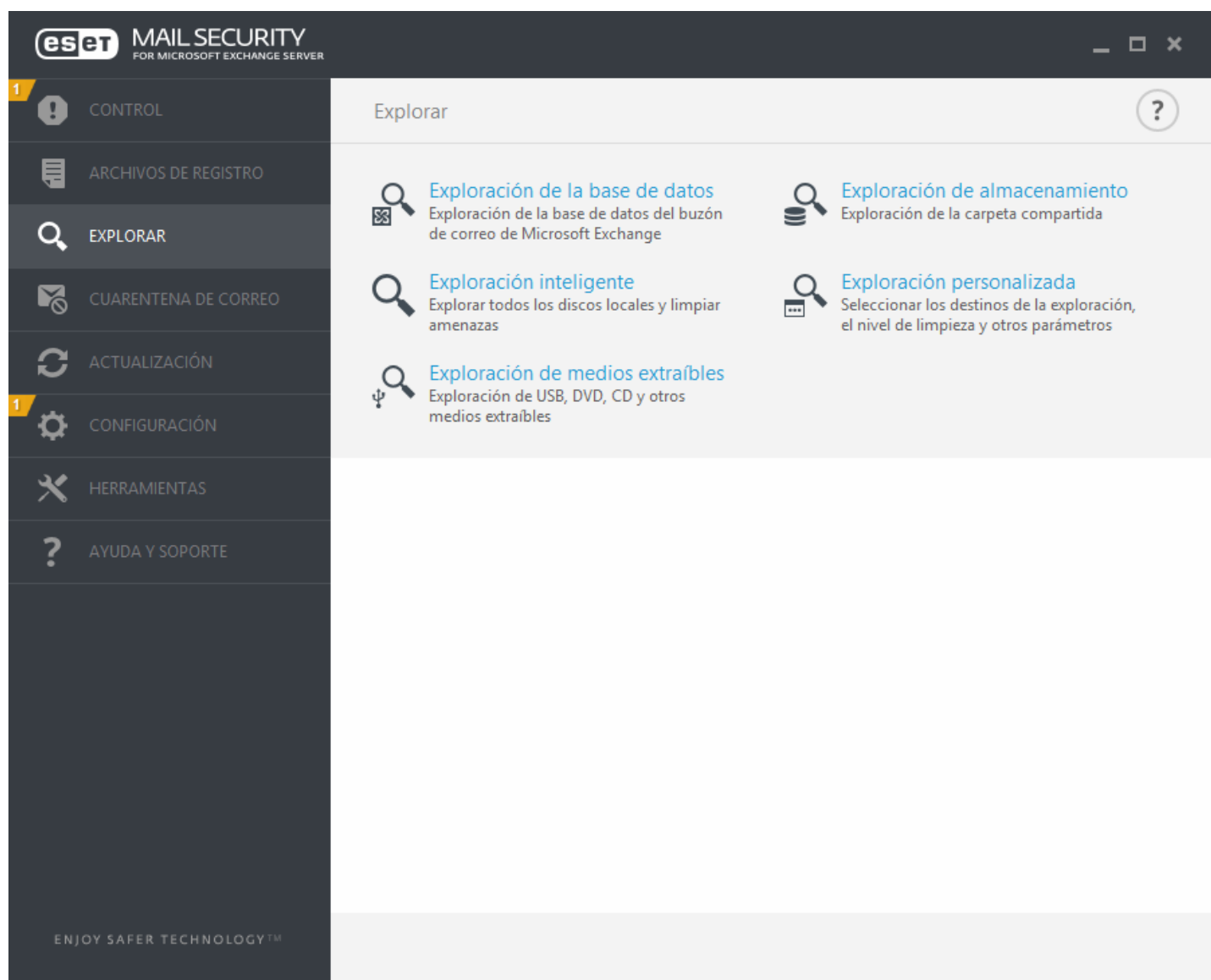
Haga clic en el ícono del interruptor ☐ **Filtrado** para abrir la ventana **Filtrado de registros** donde puede definir los [criterios de filtrado](#).

Puede hacer que el menú contextual aparezca al hacer clic con el botón secundario en un historial específico. Las siguientes opciones se encuentran disponibles en el menú contextual:

- **Filtrar registros iguales:** activa la filtración de registros y muestra solamente los registros del mismo tipo que el registro seleccionado.
- **Filtrar...:** al hacer clic en esta opción, la ventana [Filtrar registros](#) le permitirá definir los criterios de filtrado para las entradas de registro específicas.
- **Habilitar filtro:** activa las configuraciones de los filtros. La primera vez que filtre los registros, debe definir los criterios de filtrado. Una vez que los filtros están configurados, permanecerán sin cambios hasta que los edite.
- **Deshabilitar filtro:** desactiva los filtros (al igual que el hacer clic en el interruptor en la parte inferior). Esta opción se encuentra disponible solamente cuando el filtrado se encuentra habilitado.
- **Copiar:** copia la información de los registros seleccionados/resaltados al portapapeles.
- **Copiar todo:** copia la información de todos los registros que aparecen en la ventana.
- **Exportar...:** exporta la información de los registros seleccionados/resaltado a un archivo XML.
- **Exportar todo...:** exporta toda la información de la ventana a un archivo XML.
- **Buscar...:** abre la ventana [Buscar en los registros](#) y le permite definir los criterios de búsqueda. Trabaja sobre el contenido que ya se filtró como medio adicional para reducir los resultados.
- **Buscar siguiente:** busca la siguiente concordancia con la búsqueda definida con anterioridad (ver arriba).
- **Buscar anterior:** busca la concordancia anterior con la búsqueda definida con anterioridad (ver arriba).

3.3 Exploración

El módulo de exploración a petición es una parte importante de ESET Mail Security. Se usa para realizar la exploración de los archivos y las carpetas del equipo. Desde el punto de vista de la seguridad, es esencial que las exploraciones del equipo no se ejecuten solo cuando existen sospechas de una infección, sino en forma habitual como parte de una medida de seguridad de rutina. Recomendamos que realice exploraciones profundas de manera regular (por ejemplo, una vez al mes) en su sistema para detectar los virus que no haya detectado la [Protección del sistema de archivos en tiempo real](#). Esto puede ocurrir si la Protección del sistema de archivos en tiempo real se deshabilitó en algún momento, si la base de datos de virus era obsoleta o si el archivo no se detectó como virus cuando se guardó en el disco.



Se encuentran disponibles dos tipos de **Exploración del equipo**. **Exploración inteligente** explora rápidamente el sistema sin necesidad de realizar configuraciones adicionales de los parámetros de exploración. La **Exploración personalizada** le permite seleccionar cualquiera de los perfiles de exploración predefinidos y definir objetos específicos para la exploración.

Para obtener más información sobre el proceso de la exploración, consulte [Progreso de la exploración](#).

Exploración de la base de datos

Le permite ejecutar exploraciones de la base de datos a petición. Puede elegir **Carpetas públicas, servidores de correo y buzón de correo** para la exploración. Además, puede usar las [Tareas programadas](#) para ejecutar el explorador de la base de datos en un horario específico o en un evento.

¡NOTA

si ejecuta Microsoft Exchange Server 2007 o 2010 puede elegir entre la [Protección de la base de datos de correo electrónico](#) y la [Exploración de la base de datos a petición](#). No obstante, solamente uno de estos dos tipos de protección puede estar activo a la vez. Si decide utilizar la Exploración de la base de datos a petición, deberá deshabilitar la integración de la Protección de la base de datos de correo electrónico en la Configuración avanzada del [Servidor](#). De lo contrario, la **Exploración de la base de datos a petición** no estará disponible.

Exploración de almacenamiento

Explora todas las carpetas compartidas dentro del servidor local. Si **Exploración de almacenamiento** no se encuentra disponible, significa que no hay carpetas compartidas en su servidor.

Exploración de Hyper-V

Esta opción únicamente estará visible en el menú si el administrador de Hyper-V está instalado en el servidor que ejecuta ESET Mail Security. La exploración de Hyper-V permite explorar los discos de las máquinas virtuales (VM) en [Microsoft Hyper-V Server](#) sin la necesidad de tener instalado un “agente” en la VM en cuestión. Consulte [Exploración de Hyper-V](#) para obtener más información (incluidos los sistemas operativos del host compatibles y las limitaciones).

Exploración inteligente

La exploración inteligente permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja de la Exploración inteligente es su facilidad de uso y que no requiere una configuración detallada de la exploración. La exploración inteligente verifica todos los archivos en los discos locales y desinfecta o elimina en forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado. Para obtener información más detallada sobre los tipos de desinfección, consulte [Desinfección](#).

Exploración personalizada

La exploración personalizada es una solución ideal si desea especificar los parámetros de exploración, tales como los objetos para explorar y los métodos de exploración. La ventaja de la exploración personalizada es la capacidad de configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles de exploración definidos por el usuario, lo que resulta útil si la exploración se efectúa reiteradamente con el uso de los mismos parámetros.

Para elegir los objetos para explorar, seleccione **Exploración del equipo > Exploración personalizada** y seleccione una opción en el menú desplegable **Objetos para explorar** o seleccione objetos específicos desde la estructura con forma de árbol. El objeto para explorar también puede definirse mediante el ingreso de la ruta de las carpetas o archivos que desea incluir. Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Al realizar una exploración, puede elegir tres niveles de desinfección mediante un clic en **Configuración > Parámetros ThreatSense > Desinfección**.

La opción de realizar exploraciones del equipo mediante la Exploración personalizada se recomienda solo para los usuarios avanzados con experiencia previa en el uso de programas antivirus.

Exploración de medios extraíbles

Es similar a la exploración inteligente: inicia rápidamente una exploración de los medios extraíbles (como CD/DVD/USB) que estén conectados al equipo. Puede ser útil cuando conecta al equipo una unidad flash USB y desea explorar sus contenidos en busca de malware y otras amenazas potenciales.

Este tipo de exploración también puede iniciarse al hacer clic en **Exploración personalizada**, luego seleccionar **Medios extraíbles** del menú desplegable de **Objetos para explorar** y, por último, hacer clic en **Explorar**.

Repetir la última exploración

Lleva a cabo la última exploración, cualquiera haya sido (Almacenamiento, Inteligente, Personalizada, etc.), con la misma configuración.

i NOTA

repita la última función de exploración no estará disponible si la Exploración de la base de datos a petición está presente.

i NOTA

se recomienda ejecutar una exploración del equipo al menos una vez al mes. La exploración se puede configurar como una [tarea programada](#) desde **Herramientas > Tareas programadas**.

3.3.1 Exploración de Hyper-V

La exploración del antivirus de Hyper-V ofrece la capacidad de explorar los discos de un servidor [Microsoft Hyper-V Server](#), es decir, de una máquina virtual (VM) sin la necesidad de tener instalado un “agente” en la VM en cuestión. El antivirus se instala usando los privilegios de administrador del servidor Hyper-V.

Sistemas operativos compatibles del host

- Windows Server 2008 R2: Las máquinas virtuales se podrán explorar solo si están fuera de línea
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 (ESET Mail Security 6.4.12004.0)

Requisitos de hardware

El servidor no debería tener problemas de rendimiento al ejecutar las máquinas virtuales. La actividad de exploración usa principalmente recursos de la CPU.

En el caso de la exploración en línea de las VMs se necesita tener espacio libre en el disco. El espacio libre en el disco (espacio disponible para usar) debe ser de al menos el doble del espacio usado por los puntos de control/las instantáneas y por los discos virtuales.

Limitaciones específicas

- La exploración en almacenamiento RAID, volúmenes distribuidos y [Discos Dinámicos](#) no es compatible debido a la naturaleza de los Discos Dinámicos. Por lo tanto, recomendamos que evite usar el tipo de Disco Dinámico en sus VM si es posible.
- La exploración siempre se realiza solo en la Máquina Virtual actual, no afecta sus puntos de control/instantáneas.
- Actualmente, no se admite ejecutar Hyper-V en un host en un clúster con ESET Mail Security.
- Las máquinas virtuales en un host de Hyper-V que se ejecutan en Windows Server 2008 R2 solo pueden explorarse en modo solo lectura (**Sin desinfección**), sin importar el nivel de desinfección seleccionado en los parámetros de [ThreatSense](#).

i NOTA

La actividad de exploración usa principalmente recursos de la CPU. Mientras que ESET Security es compatible con la exploración de MBR de disco virtual, el único método compatible es la exploración de solo lectura. Esta configuración puede cambiarse en **Configuración avanzada > Antivirus > Exploración de Hyper-V > [parámetros de ThreatSense](#) > Sectores de inicio**.

La máquina virtual que se va a explorar está “desconectada” (apagada)

ESET Mail Security usa el administrador de Hyper-V para detectar y conectarse a los discos virtuales. De este modo, ESET Mail Security tiene el mismo acceso al contenido de los discos virtuales que si estuviera accediendo a los datos y a los archivos de cualquier unidad genérica.

La máquina virtual que se va a explorar está “conectada” (se está ejecutando, está en pausa, guardada)

ESET Mail Security usa administrador de Hyper-V para detectar los discos virtuales de las máquinas virtuales. La conexión real a estos discos no es posible. Por lo tanto, ESET Mail Security crea un punto de control/una instantánea de la máquina virtual, y luego se conecta al punto de control/a la instantánea. Una vez finalizada la exploración, se elimina el punto de control/la instantánea. Esto significa que la exploración de solo lectura se puede llevar a cabo

porque la actividad de la exploración no afecta la ejecución de las Máquinas virtuales.

La creación de un punto de control/una instantánea es una operación lenta y podría tardar unos pocos segundos hasta un minuto. Debe tener esto en cuenta cuando planea ejecutar una exploración de Hyper-V en una gran cantidad de máquinas virtuales.

Convención de nomenclatura

El módulo de exploración de Hyper-V usa la siguiente convención de nomenclatura:

`VirtualMachineName\DiskX\VolumeY`

donde X es el número de disco e Y es el número de volumen.

Por ejemplo, "Computer\Disk0\Volume1".

El sufijo de número se añade basándose en el orden de detección, que es idéntico al orden que se ve en el Administrador de discos de la VM.

Esta convención de nombres se usa en la lista de estructura de árbol de objetivos que se analizarán, en la barra de progreso y también en los archivos de registro.

Ejecución de una exploración

La exploración se podrá ejecutar de 3 maneras distintas:

- A petición: si hace clic en la opción Exploración de Hyper-V en el menú de ESET Mail Security, verá un listado de máquinas virtuales disponibles (si las hubiera) que podrá explorar. Es una lista de estructura de árbol, donde la entidad de nivel más bajo que se va a explorar es un volumen, es decir, no es posible seleccionar sólo un directorio o un archivo para escáner, sino que por lo menos tendrá que explorar todo el volumen. Para listar los volúmenes disponibles es necesario conectarse con el disco o con los discos virtuales en particular y esto puede tardar unos segundos. Por lo tanto, una opción más rápida es marcar la máquina virtual o los discos que se desean explorar. Una vez que haya marcado las máquinas virtuales, los discos o los volúmenes que desea explorar, haga clic en el botón Explorar.
- A través del [Programador de tareas](#)
- A través de ESET Remote Administrator como una tarea de cliente llamada Exploración del servidor.

Es posible ejecutar varias exploraciones de Hyper-V simultáneamente.

Una vez finalizada la exploración, verá una notificación y un enlace de Mostrar registro por el cual podrá revisar los detalles de la exploración realizada. Todos los registros de exploración están disponibles en la sección de Archivos de registro de ESET Mail Security, pero tendrá que seleccionar la exploración de Hyper-V en el menú desplegable para ver los registros relacionados.

Problemas posibles

- Al ejecutar la exploración de una máquina virtual en línea, se deberá generar un punto de control/una instantánea de la máquina virtual que se desea explorar, y durante la creación del punto de control/de la instantánea algunas acciones genéricas de la máquina virtual podrán verse limitadas o estar deshabilitadas.
- Si se está explorando una máquina virtual sin conexión, no podrá encender la VM hasta que haya finalizado la exploración.
- El administrador de Hyper-V permite nombrar usando el mismo nombre a dos Máquinas virtuales diferentes y esto representa un problema cuando se trata de identificar las máquinas, al revisar los registros de exploración.

3.4 Cuarentena de correo

El administrador de Cuarentena de correo electrónico está disponible para los tres tipos de cuarentena:

- [Cuarentena local](#)
- [Correo electrónico de cuarentena](#)
- [Cuarentena de MS Exchange](#)

i NOTA

Si el administrador de cuarentena del correo está en gris, se debe a las siguientes razones. Se está ejecutando Microsoft Exchange Server 2003 y esta característica no es compatible o EWS (Exchange Web Services) no está disponible. Esto no se aplica a la [cuarentena local](#), la cuarentena local funcionará con todos los Exchange Servers e independientemente de la disponibilidad de EWS.

i NOTA


la [interfaz web de la Cuarentena de correo](#) es un administrador alternativo de la Cuarentena de correo que le permite administrar los objetos de correo electrónico en cuarentena.

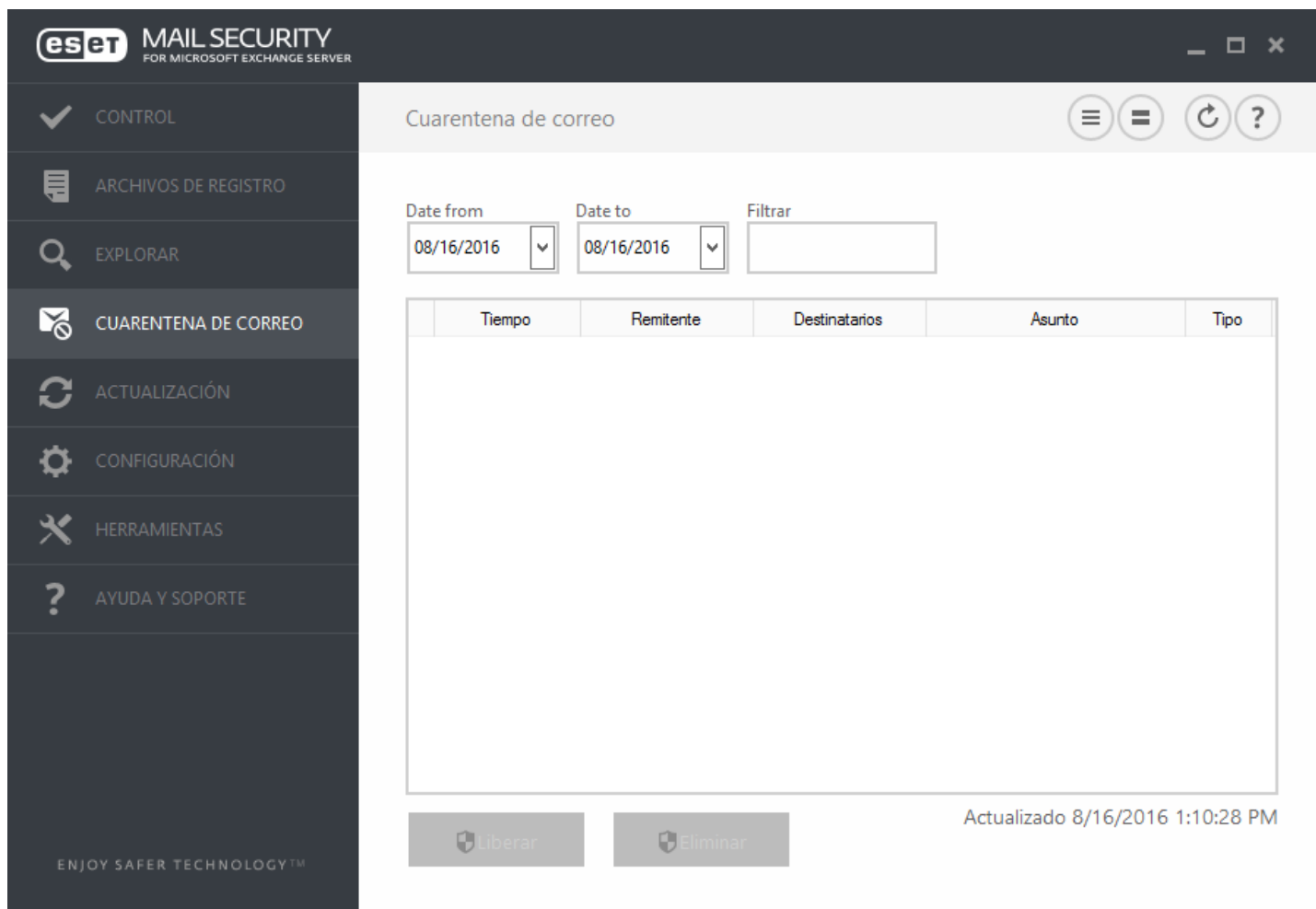
Filtrado

Seleccione intervalo (**Fecha desde** y **Fecha hasta**) para filtrar los correos electrónicos en cuarentena.

Filtro: ingrese una cadena en el cuadro de texto para filtrar los correos electrónicos que se muestran (se busca todas las columnas).

i NOTA

los datos del administrador de Cuarentena de correo no se actualizan de manera automática, recomendamos hacer clic en actualizar  de manera periódica para ver los elementos más actuales en la Cuarentena de correo.



Acción

Liberar: libera los correos electrónicos a los destinatarios originales mediante el directorio de reproducción nueva y los elimina de la cuarentena. Haga clic en **Sí** para confirmar la acción.

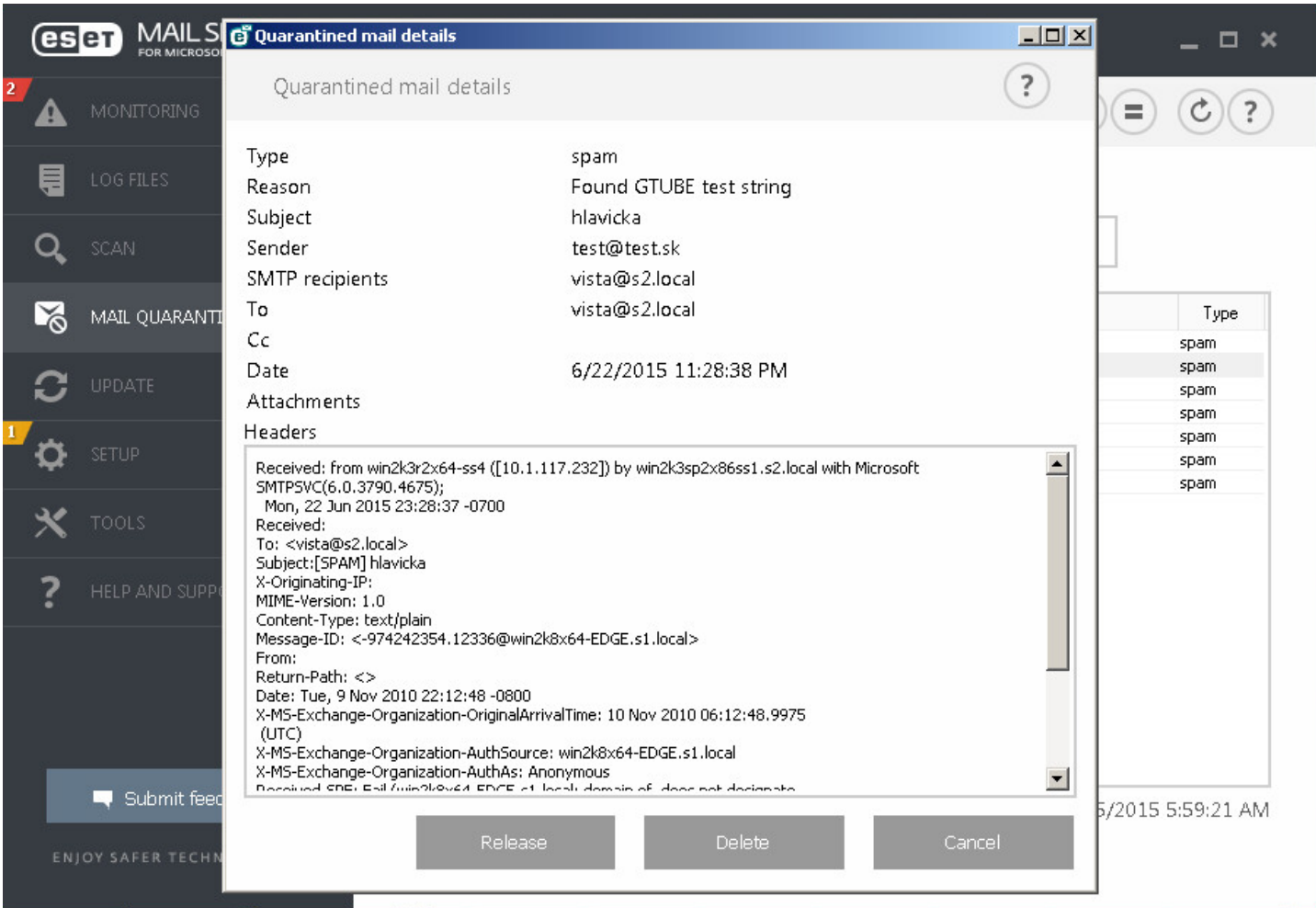
i NOTA

Cuando se libera un correo de cuarentena, ESET Mail Security ignora el encabezado **To:** MIME porque se puede alterar fácilmente. En cambio, usa la información del destinatario original del comando **RCPT TO:** adquirida durante la conexión de SMTP. De esta manera, se garantiza que el destinatario correcto del correo reciba el mensaje liberado de cuarentena.

Eliminar: elimina el elemento de la cuarentena. Haga clic en **Sí** para confirmar la acción.

Poner en cuarentena detalles de correo: haga doble clic en el mensaje en cuarentena o clic con el botón secundario y seleccione **Detalles**, se abrirá una ventana emergente con detalles sobre el mensaje de correo electrónico en cuarentena. También puede encontrar información adicional sobre el correo electrónico en el encabezado de correo electrónico RFC.

Las acciones también están disponibles en el menú contextual. Si lo desea, haga clic en **Liberar**, **Eliminar** o **Eliminar de manera permanente** para realizar una acción sobre un mensaje de correo electrónico en cuarentena. Haga clic en **Sí** para confirmar la acción. Si elige **Eliminar de manera permanente** el mensaje se eliminará también del sistema de archivos, a la inversa que **Eliminar** que eliminará el elemento de la vista del administrador de la Cuarentena de correo.



3.4.1 Detalles del correo en cuarentena

Esta ventana contiene información sobre el mensaje de correo electrónico en cuarentena como **Tipo**, **Motivo**, **Asunto**, **Remitente**, **Destinatarios SMTP**, **Para**, **Cc**, **Fecha**, **Adjuntos** y **Encabezados**. Puede seleccionar, copiar y pegar los encabezados si así lo necesita.

Puede realizar una acción con los mensajes de correo electrónico en cuarentena utilizando los botones:

- **Liberar**: libera los correos electrónicos a los destinatarios originales mediante el directorio de reproducción nueva y los elimina de la cuarentena. Haga clic en **Sí** para confirmar la acción.
- **Eliminar**: elimina el elemento de la cuarentena. Haga clic en **Sí** para confirmar la acción.

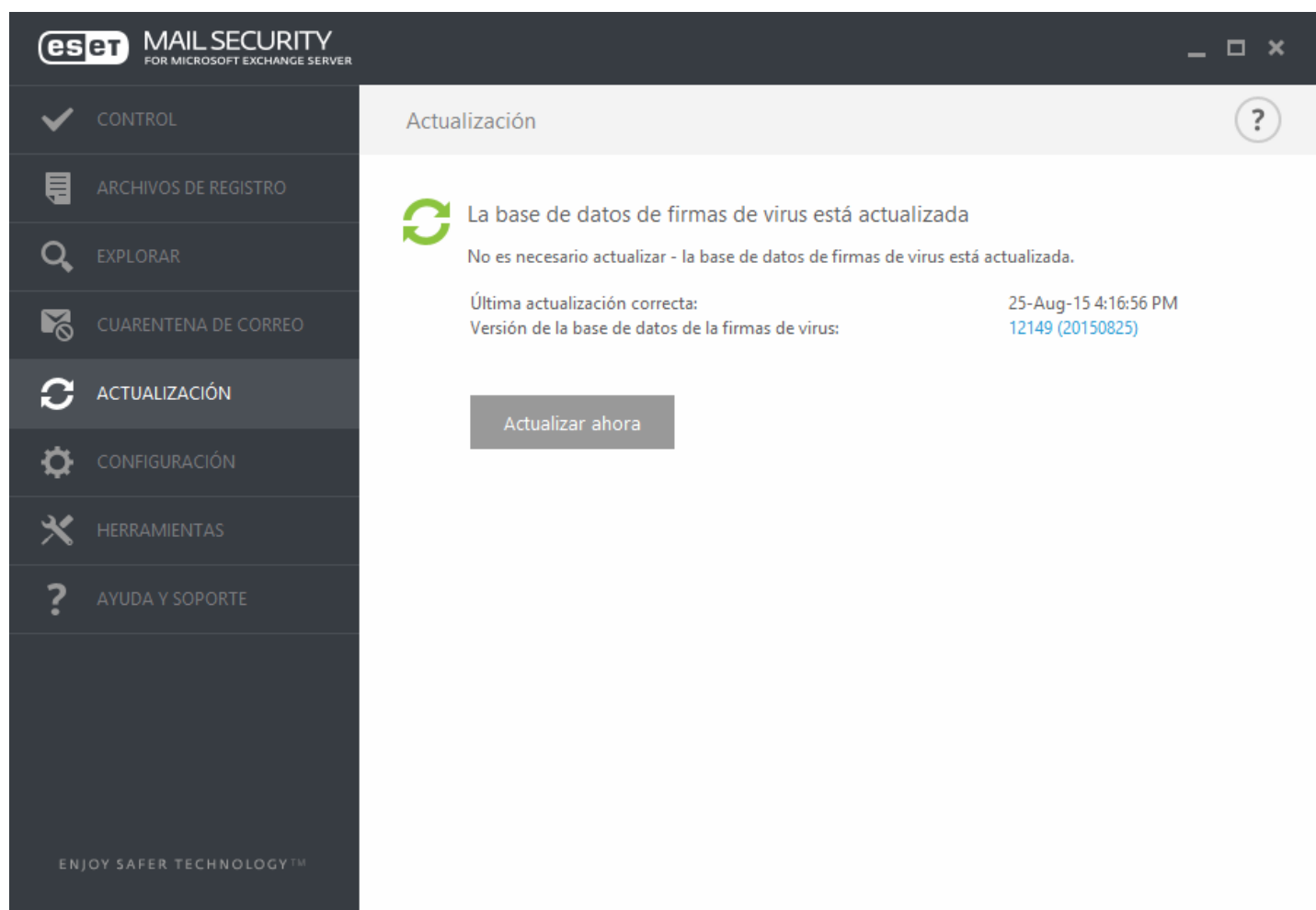
Hacer clic en el botón **Cancelar** cerrará la ventana de detalles de los Correos electrónicos en cuarentena.

3.5 Actualización

La actualización habitual de ESET Mail Security es la mejor forma de mantener el máximo nivel de seguridad en el equipo. El módulo de actualización garantiza que el programa esté siempre al día de dos maneras: actualizando la base de datos de firmas de virus y los componentes del sistema.

Al hacer clic en **Actualización** en la ventana principal del programa, encontrará el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar. La ventana principal también contiene la versión de la base de datos de firmas de virus. Este indicador numérico es un vínculo activo al sitio web de ESET, donde aparece una lista de todas las firmas agregadas en esa actualización en particular.

Haga clic en **Actualizar ahora** para comprobar si hay actualizaciones. La actualización de la base de datos de firmas de virus así como la actualización de componentes del programa constituyen una parte fundamental para mantener una protección completa contra códigos maliciosos.



Última actualización correcta: es la fecha de la última actualización. Asegúrese de que la fecha sea reciente, lo que significa que la base de datos de firmas de virus está al día.

Versión de la base de datos de firmas de virus: el número de la base de datos de firmas de virus, que además es un enlace activo al sitio web de ESET. Haga clic para ver una lista de todas las firmas agregadas en una actualización en particular.

Proceso de actualización

Luego de hacer clic en **Actualizar ahora**, comienza el proceso de descarga y se muestra el progreso de la actualización. Para interrumpir la actualización, haga clic en **Cancelar actualización**.

IMPORTANTE

en circunstancias normales, cuando las actualizaciones se descargan correctamente, aparecerá el mensaje **No es necesario actualizar: la base de datos de firmas de virus está actualizada** en la ventana **Actualización**. Si este no es

el caso, el programa está desactualizado y más vulnerable a una infección. Actualice la base de datos de firmas de virus lo antes posible. De lo contrario, se mostrará uno de los siguientes mensajes:

La base de datos de firmas de virus está desactualizada: este error aparecerá luego de varios intentos fallidos de actualizar la base de datos de firmas de virus. Es recomendable verificar la configuración de la actualización. El motivo más común de este error es el ingreso incorrecto de los datos de autenticación o la configuración incorrecta de las [opciones de conexión](#).

La notificación anterior está relacionada con los dos mensajes siguientes **Falló la actualización de la base de datos de firmas de virus** sobre actualizaciones insatisfactorias que se detallan a continuación:

Licencia no válida: la clave de licencia no se ha ingresado correctamente en la configuración de actualización. Es recomendable que compruebe sus datos de autenticación. La ventana de Configuración avanzada (presione la tecla F5 de su teclado) contiene opciones de actualización adicionales. Haga clic en **Ayuda y soporte > Administrar licencia** en el menú principal para ingresar una clave de licencia nueva.

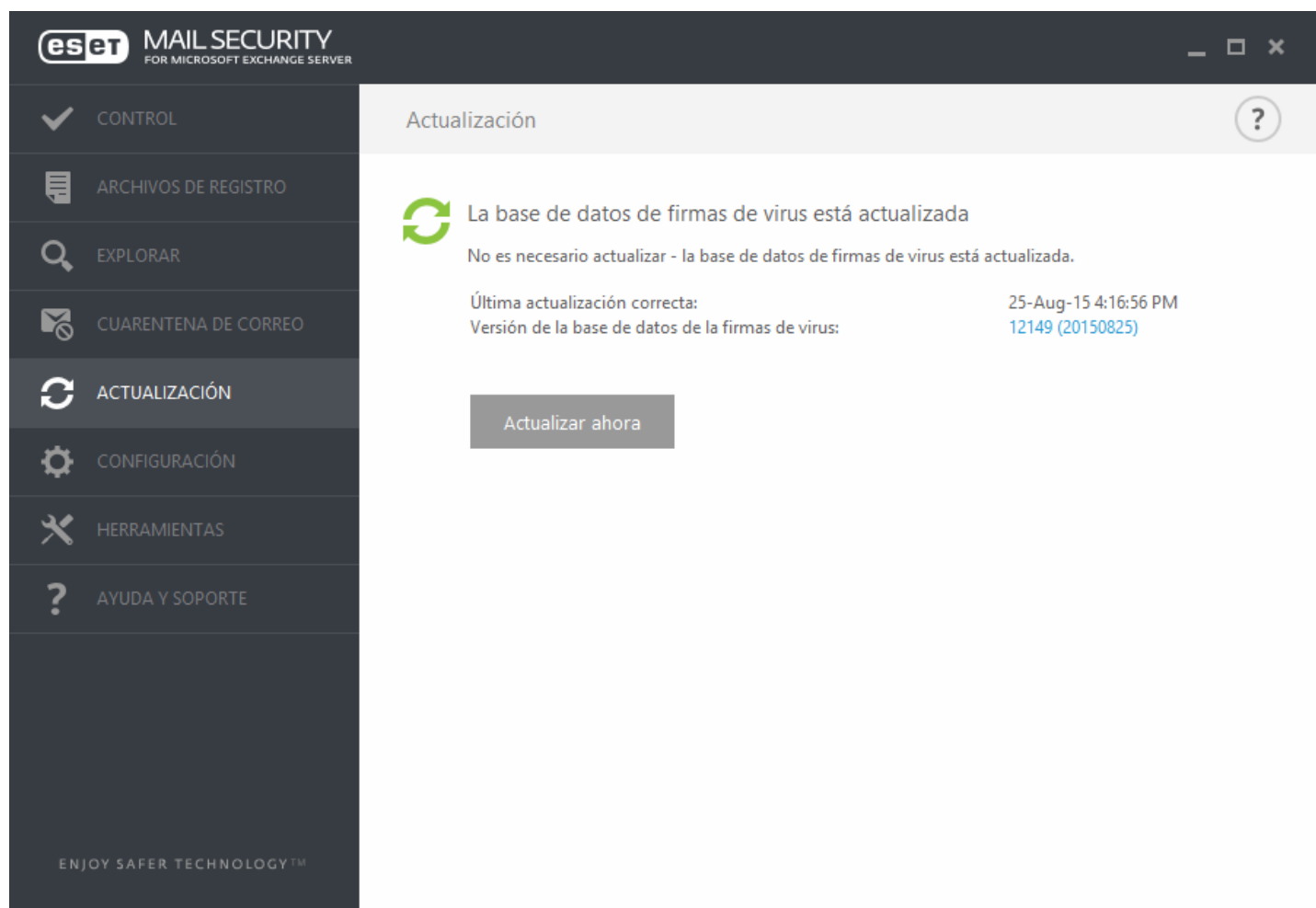
Se produjo un error al descargar los archivos de actualización: una causa posible de este error es la [configuración de la conexión a Internet](#) incorrecta. Es recomendable verificar su conectividad a Internet; para ello, abra cualquier sitio web en su navegador. Si el sitio web no se abre, es probable que la conexión a Internet no esté establecida o que haya problemas de conectividad en el equipo. Consulte el problema con su proveedor de servicios de Internet (ISP) si su conexión está inactiva.

NOTA

Para obtener más información, visite este artículo de la [Base de conocimiento de ESET](#).

3.5.1 Configurar la actualización de DB de virus

La actualización de la base de datos de firmas de virus y de los componentes del programa constituye una parte fundamental para proporcionar una protección completa contra códigos maliciosos. Preste suma atención a su configuración y funcionamiento. Desde el menú principal, seleccione **Actualizar** y luego haga clic en **Actualizar ahora** para verificar si hay una actualización de la base de datos de firmas.



Puede configurar las opciones de actualización en la ventana de configuración avanzada (presione la tecla F5 de su teclado). Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy, las conexiones de LAN y la configuración de copias de firmas de virus (mirror), haga clic en **Actualizar** en la ventana de **Configuración avanzada** a la izquierda. En caso de que surjan problemas con una actualización, haga clic en **Borrar caché** para borrar la carpeta de actualización temporal. El menú **Servidor de actualización** está configurado en **SELECCIONAR AUTOMÁTICAMENTE** en forma predeterminada. **SELECCIONAR AUTOMÁTICAMENTE** significa que el servidor de actualización, desde el cual se van a descargar las actualizaciones de firmas de virus, se selecciona en forma automática. Recomendamos que deje seleccionada la opción predeterminada. Si no desea que aparezca la notificación de la bandeja del sistema en el sector inferior derecho de la pantalla, seleccione **Deshabilitar mostrar notificación acerca de actualización correcta**.

The screenshot shows the 'Configuración avanzada' (Advanced Configuration) window. On the left is a sidebar with navigation options: SERVIDOR, EQUIPO, ACTUALIZACIÓN (highlighted in blue), INTERNET Y CORREO ELECTRÓNICO, CONTROL DEL DISPOSITIVO, HERRAMIENTAS, and INTERFAZ DEL USUARIO. The main area is titled 'GENERAL' and contains the following settings:

- Perfil seleccionado:** A dropdown menu set to 'Mi perfil'.
- Lista de perfiles:** A link labeled 'Editar'.
- Borrar caché de actualización:** A blue button labeled 'Borrar'.
- ALERTAS DE BASE DE DATOS DE FIRMAS DE VIRUS OBSOLETA:** A section with a description: 'Esta configuración define la antigüedad máxima permitida para la base de datos de firmas de virus antes de que se considere obsoleta, y una alerta se mostrará.'
 - Establecer una antigüedad máxima para la base de datos automáticamente:** A toggle switch that is turned on (blue).
 - Edad máxima para la base de datos (días):** A numeric input field set to '7'.
- REVERSIÓN:** A section with two settings:
 - Crear instantáneas de archivos actualizados:** A toggle switch that is turned on (blue).
 - Número de instantáneas almacenadas localmente:** A numeric input field set to '2'.

At the bottom of the window, there are three buttons: 'Predeterminado' (gray), 'Aceptar' (blue with a shield icon), and 'Cancelar' (gray).

Para un funcionamiento óptimo, es importante que el programa se actualice automáticamente. Esto solo será posible si se ingresa la **Clave de licencia** correcta en **Ayuda y soporte > Activar la licencia**.

Si no activó su producto luego de la instalación, puede hacerlo en cualquier momento. Para obtener información más detallada acerca de la activación, consulte el apartado [Cómo activar ESET Mail Security](#) e ingrese los datos de la licencia que recibió con su producto de seguridad ESET en la ventana "Detalles de la licencia".

3.5.2 Configurar el servidor proxy para actualizaciones

Si usa un servidor proxy para la conexión a Internet en el sistema donde ESET Mail Security está instalado, debe configurarlo desde “Configuración avanzada”. Para acceder a la ventana de configuración del servidor proxy, presione la tecla F5 para abrir la ventana de configuración avanzada y haga clic en **Actualizar > Proxy HTTP**. Seleccione **Conexión a través de un servidor proxy** del menú desplegable **Modo de proxy** y complete los detalles de su servidor proxy: **Servidor proxy** (dirección IP), número de **Puerto** y **Nombre de usuario** y **Contraseña** (si corresponde).

The screenshot shows the 'Configuración avanzada' (Advanced Configuration) window. On the left is a sidebar with categories: SERVIDOR, EQUIPO, ACTUALIZACIÓN (highlighted in blue), INTERNET Y CORREO ELECTRÓNICO, CONTROL DEL DISPOSITIVO, HERRAMIENTAS, and INTERFAZ DEL USUARIO. The main area displays a list of configuration sections: BÁSICO, MODO DE ACTUALIZACIÓN, PROXY HTTP (expanded), PERSONALIZAR SERVIDOR PROXY, CONECTARSE A LA LAN COMO, and REPLICACIÓN. The 'PROXY HTTP' section is active, showing a 'Modo proxy' dropdown menu set to 'Usar la configuración gl...'. Below this, the 'PERSONALIZAR SERVIDOR PROXY' section contains four input fields: 'Servidor proxy', 'Puerto' (with the value 3128), 'Nombre de usuario', and 'Contraseña'. Each field has an information icon (i) to its right. At the bottom of the window are three buttons: 'Predeterminado', 'Aceptar' (with a shield icon), and 'Cancelar'.

Si no está seguro de los detalles del servidor proxy, puede tratar de detectar automáticamente la configuración de su servidor proxy mediante la selección de **Usar la configuración global del servidor proxy** de la lista desplegable.

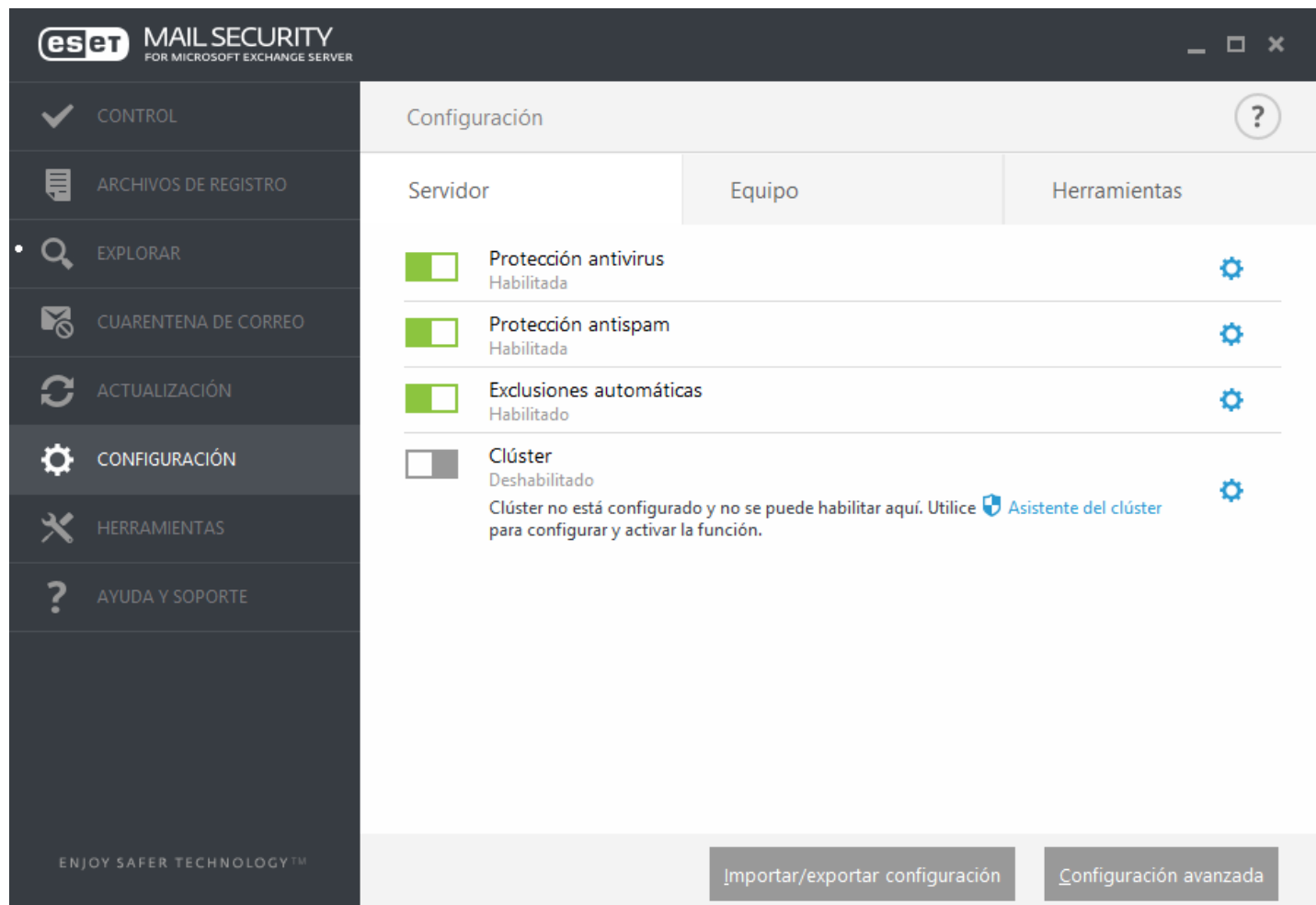
i NOTA


es posible que las opciones del servidor proxy para distintos perfiles de actualización difieran entre sí. En este caso, configure los distintos perfiles de actualización en la configuración avanzada con un clic en **Actualización > Perfil**.


3.6 Configuración


El menú **Configuración** contiene las siguientes secciones:

- [Servidor](#)
- [Equipo](#)
- [Herramientas](#)



Para deshabilitar temporalmente los módulos individuales, haga clic en el interruptor verde  junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del equipo.



Para volver a habilitar la protección de un componente de seguridad deshabilitado, haga clic en el interruptor rojo  para regresar un componente a su estado de habilitado.

Para acceder a configuraciones detalladas para un componente de seguridad específico, haga clic en icono de engranaje .

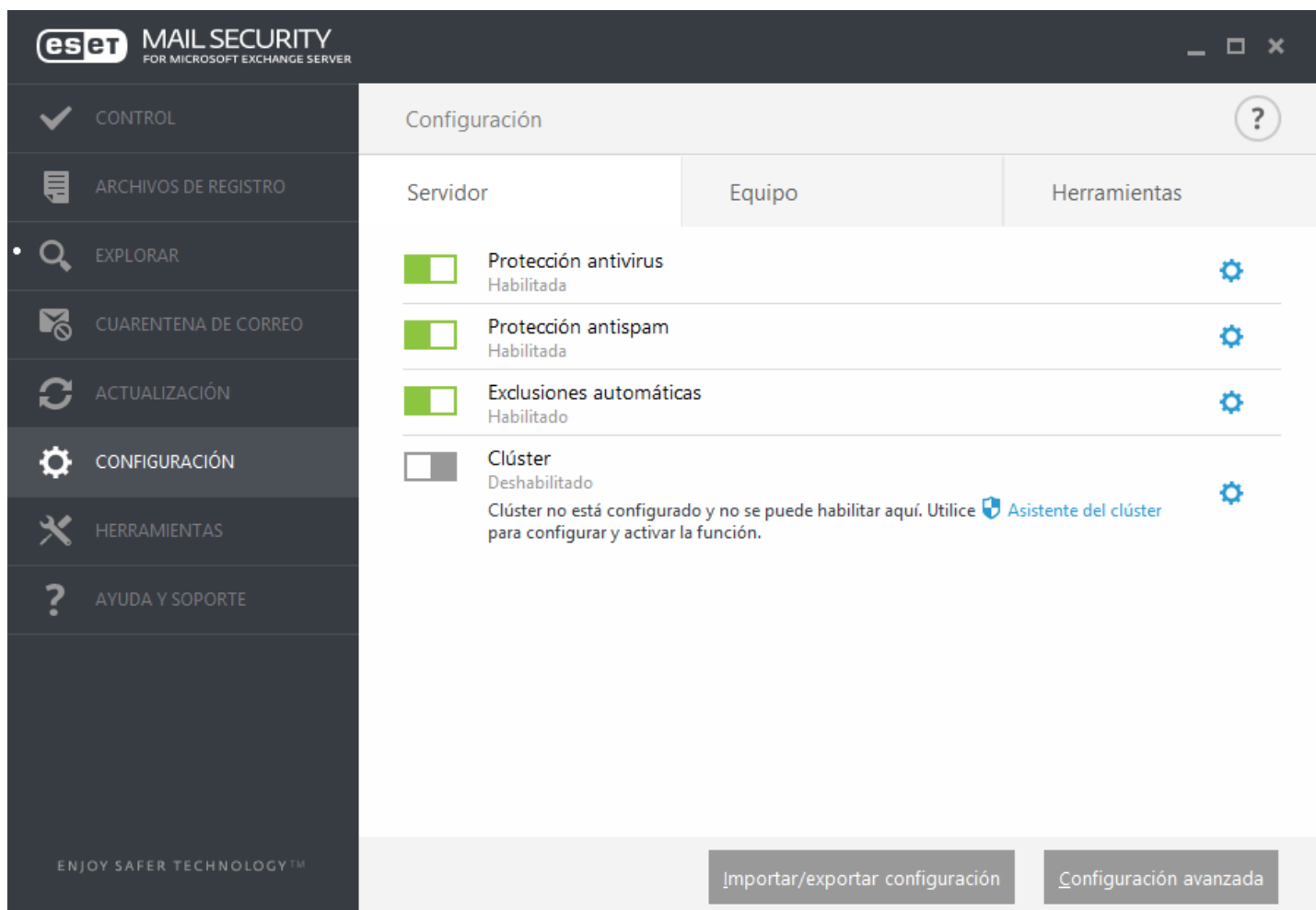
Si desea establecer opciones más detalladas, haga clic en **Configuración avanzada** o presione la tecla **F5**.






Hay opciones adicionales en la parte inferior de la ventana de configuración. Para cargar los parámetros de configuración mediante un archivo de configuración **.xml** o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción **Importar/Exportar configuraciones**. Consulte [Importar/Exportar configuraciones](#) para obtener información más detallada.

3.6.1 Servidor

Verá una lista de componentes que puede habilitar o deshabilitar con el interruptor . Para configurar los ajustes para un elemento específico, haga clic en la rueda dentada .

- **Protección antivirus:** defiende el sistema ante ataques malintencionados mediante el control de archivos, correos electrónicos y comunicaciones por Internet.
- **Protección antispam:** integra varias tecnologías (tales como RBL, DNSBL, huellas digitales, verificación de reputación, análisis de contenido, filtro bayesiano, reglas, creación manual de listas blancas y negras, etc.) para alcanzar el nivel máximo de detección de amenazas por correo electrónico.
- La característica [Exclusiones automáticas](#) identifica las aplicaciones del servidor críticas y los archivos del sistema operativo críticos, y los agrega automáticamente a la lista de [Exclusiones](#). Esta funcionalidad ayuda a minimizar el riesgo de conflictos potenciales e incrementar el rendimiento general del servidor mientras se ejecuta un software antivirus.
- Para configurar el Clúster de ESET haga clic en el **Asistente de clúster**. Para obtener detalles acerca de cómo configurar el Clúster de ESET con el asistente, haga clic [aquí](#).





Servidor	Equipo	Herramientas
<input checked="" type="checkbox"/> Protección antivirus Habilitada		
<input checked="" type="checkbox"/> Protección antispam Habilitada		
<input checked="" type="checkbox"/> Exclusiones automáticas Habilitado		
<input type="checkbox"/> Clúster Deshabilitado Clúster no está configurado y no se puede habilitar aquí. Utilice  Asistente del clúster para configurar y activar la función.		

Si desea establecer opciones más detalladas, haga clic en **Configuración avanzada** o presione la tecla **F5**.

Hay opciones adicionales en la parte inferior de la ventana de configuración. Para cargar los parámetros de configuración mediante un archivo de configuración *.xml* o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción **Configuraciones de importar/exportar**. Consulte [Configuraciones de importar/exportar](#) para obtener información más detallada.

3.6.2 Equipo

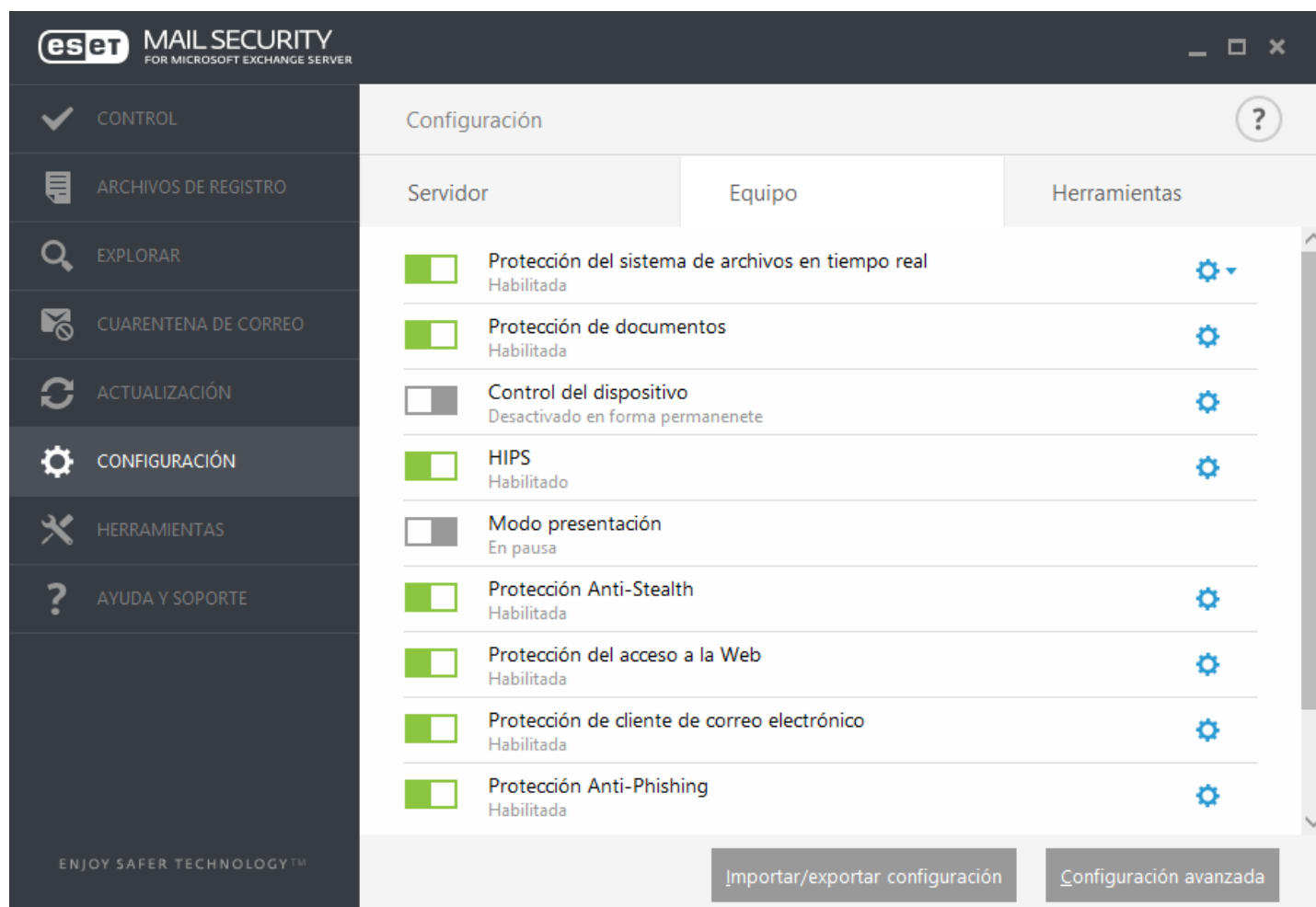
ESET Mail Security tiene todos los componentes necesarios para garantizar la protección significativa del servidor como un equipo. Cada componente proporciona un tipo específico de protección, como: Antivirus y antispyware, protección del sistema de archivos en tiempo real, acceso web, cliente de correo electrónico, protección antiphishing, etc.

La sección **Equipo** se puede encontrar en **Configuración > Equipo**. Verá una lista de los componentes que puede habilitar o deshabilitar con el interruptor . Para configurar los ajustes para un elemento específico, haga clic en la rueda dentada .

Para la **Protección del sistema de archivos en tiempo real**, también hay una opción para **Editar exclusiones**, que abrirá la ventana de configuración [Exclusiones](#) donde puede excluir archivos y carpetas de la exploración.

Detener la protección antivirus y antispyware: cuando deshabilite temporalmente la protección antivirus y antispyware, puede seleccionar el periodo de tiempo por el que desea que el componente seleccionado esté deshabilitado mediante el uso del menú desplegable y, luego, haga clic en **Aplicar** para deshabilitar el componente de seguridad. Para volver a habilitar la protección, haga clic en **Habilitar la protección antivirus y antispyware**.

El módulo **Equipo** le permite habilitar o deshabilitar y configurar los siguientes componentes:



- **Protección del sistema de archivos en tiempo real** : se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan en el equipo.
- **Protección de documentos**: la función para la protección de documentos explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer, por ej., los elementos ActiveX de Microsoft.

NOTA

la protección de documentos se encuentra deshabilitada por defecto. Si así lo desea, puede habilitarla fácilmente haciendo clic en el ícono del interruptor.


- **Control del dispositivo:** este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado.
- **HIPS:** el sistema [HIPS](#) monitorea los sucesos que ocurren dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.
- **Modo presentación:** una función para los usuarios que requieren usar el software en forma ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. Recibirá un mensaje de advertencia (riesgo potencial en la seguridad) y la ventana principal del programa se pondrá de color naranja una vez habilitado el [Modo presentación](#).
- **Protección Anti-Stealth:** proporciona la detección de programas peligrosos como los [rootkits](#), que tienen la capacidad de ocultarse del sistema operativo. Esto significa que no es posible detectarlos mediante técnicas de evaluación comunes.
- **Protección del acceso a la Web:** si se encuentra habilitada, se explora todo el tráfico que pase a través de HTTP o HTTPS en busca de software malintencionado.
- **Protección del cliente de correo electrónico:** supervisa las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing:** lo protege de sitios web ilegítimos disfrazados de legítimos que intentan obtener contraseñas, datos bancarios y demás información confidencial.

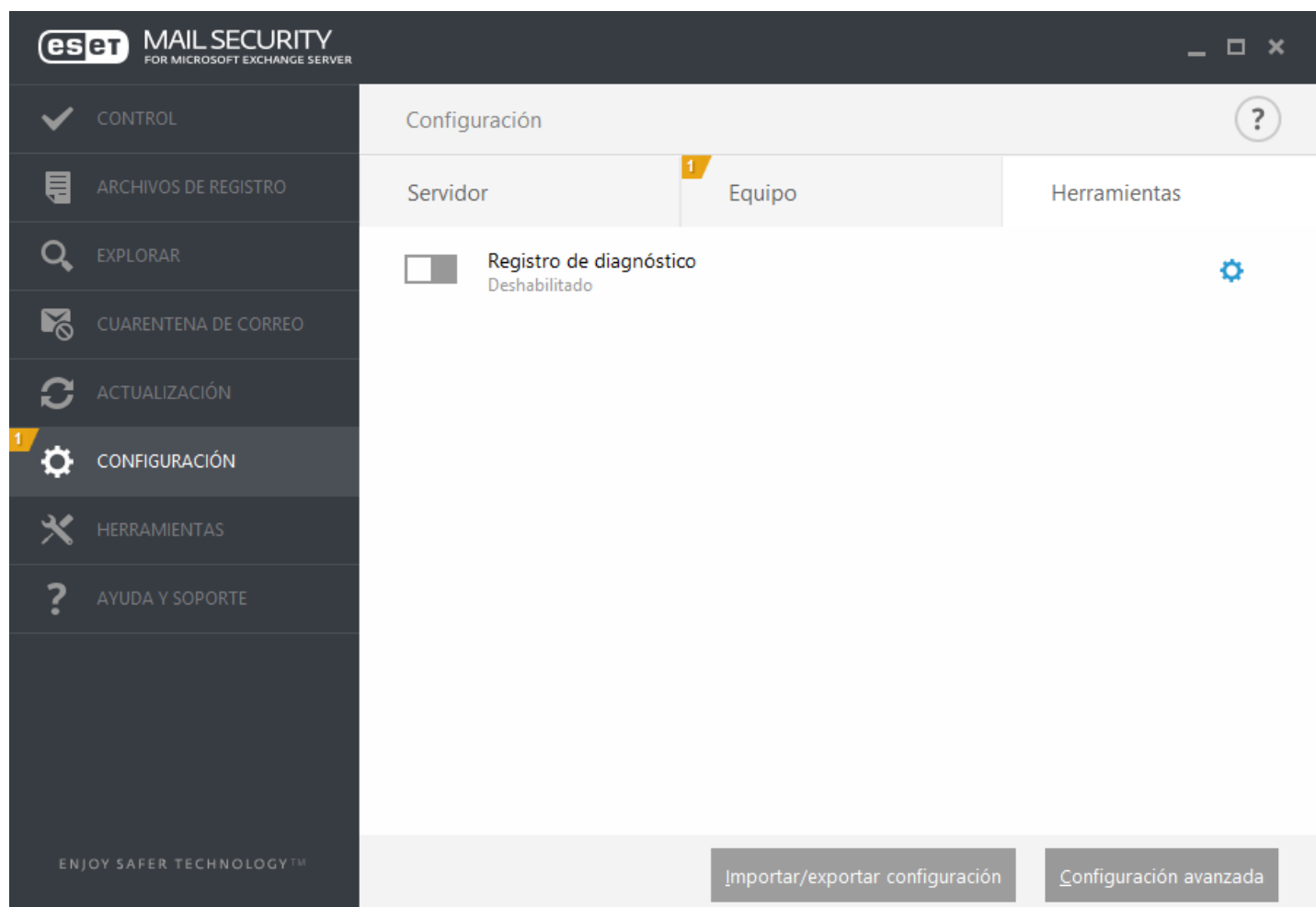
Hay opciones adicionales en la parte inferior de la ventana de configuración. Para cargar los parámetros de configuración mediante un archivo de configuración *.xml* o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción **Importar/Exportar configuraciones**. Consulte [Importar/Exportar configuraciones](#) para obtener información más detallada.

Si desea establecer opciones más detalladas, haga clic en **Configuración avanzada** o presione la tecla **F5**.

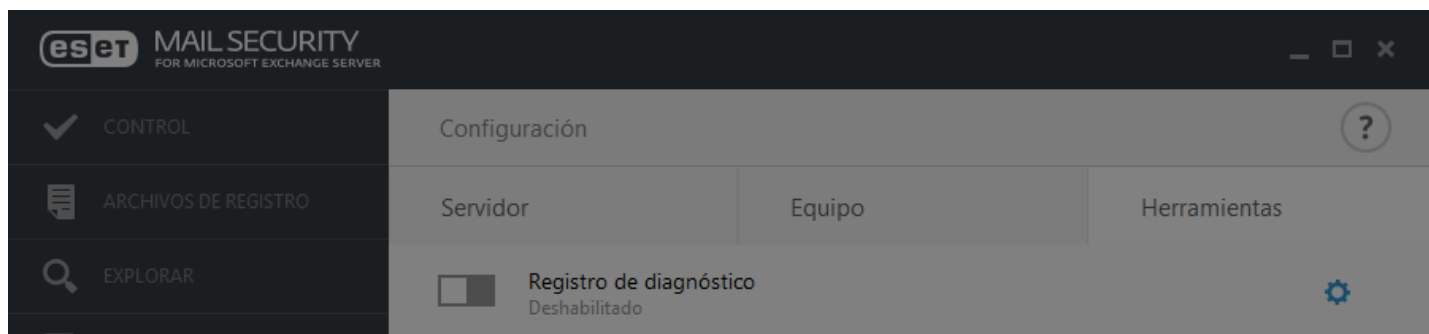
3.6.3 Herramientas

Registro de diagnóstico: al hacer clic en el interruptor para habilitar el registro de diagnóstico, podrá elegir por cuánto tiempo estará habilitado (10 minutos, 30 minutos, 1 hora, 4 horas, 24 horas, hasta el próximo reinicio del servidor o permanentemente).

Cuando hace clic en el icono del engranaje , se abrirá la ventana de Configuración avanzada en la que puede configurar los componentes que escribirán en los registros de diagnóstico cuando el registro de diagnóstico esté habilitado.

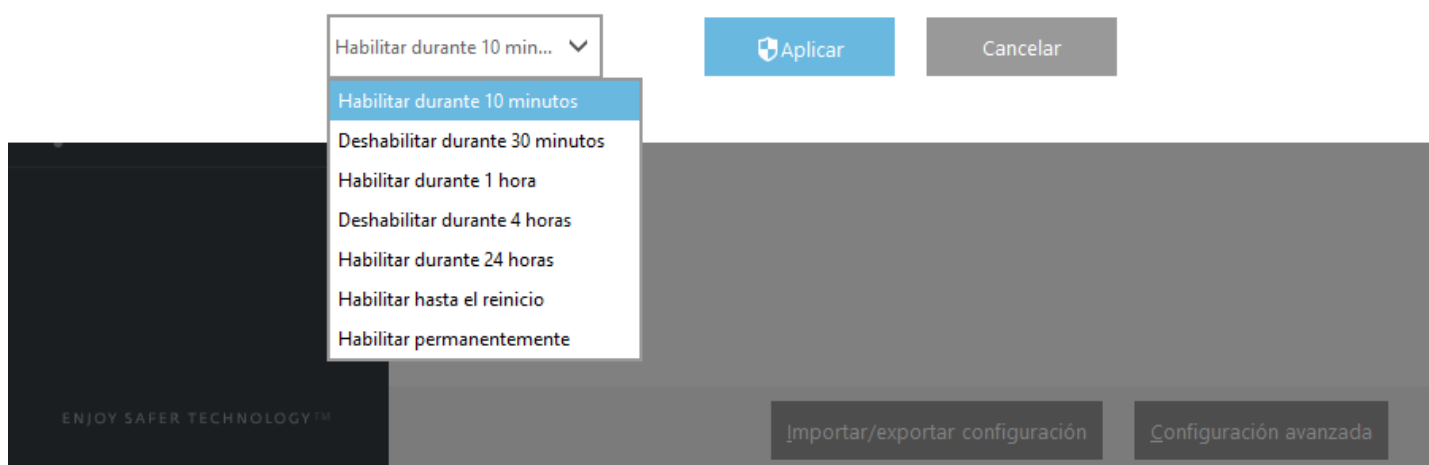


- **Habilitar** el registro de diagnóstico durante el período de tiempo seleccionado.



¿Habilitar el registro de diagnóstico?

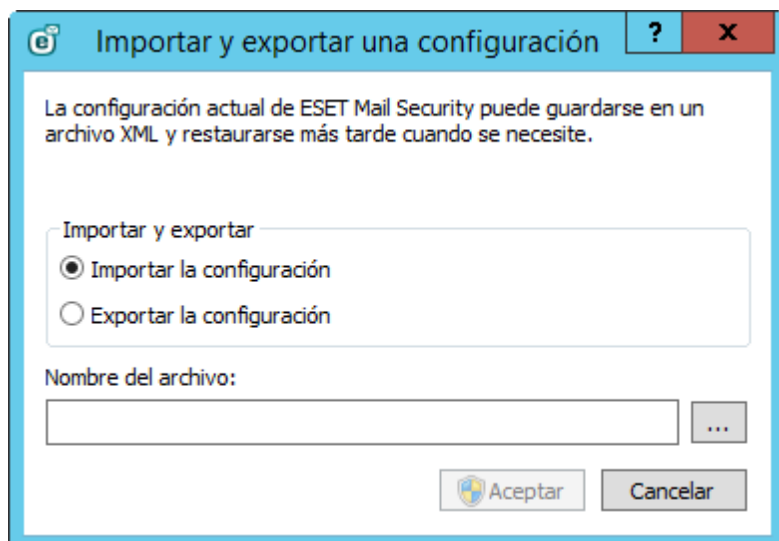
Habilitar el registro de diagnóstico durante el período de tiempo seleccionado.



3.6.4 Importación y exportación de una configuración

La importación y exportación de la configuración de ESET Mail Security está disponible en **Configuración** haciendo clic en la **Configuración Importar/Exportar**.

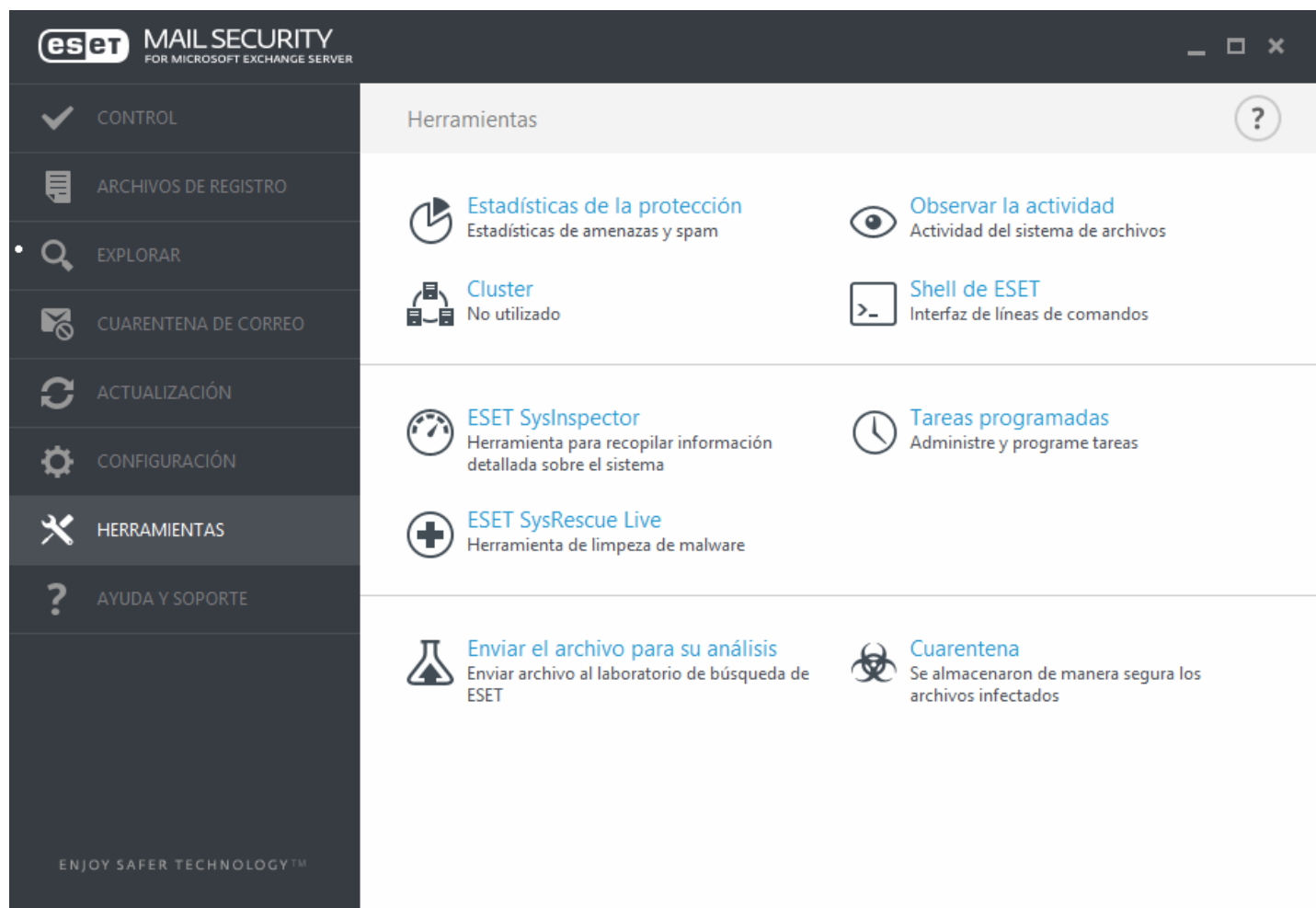
Tanto la función de importar como la de exportar usan el tipo de archivo .xml. La opción de importación y exportación es útil si necesita hacer una copia de seguridad de la configuración actual de ESET Mail Security. Se puede usar más adelante para aplicar la misma configuración a otro equipo u otros equipos.



3.7 Herramientas

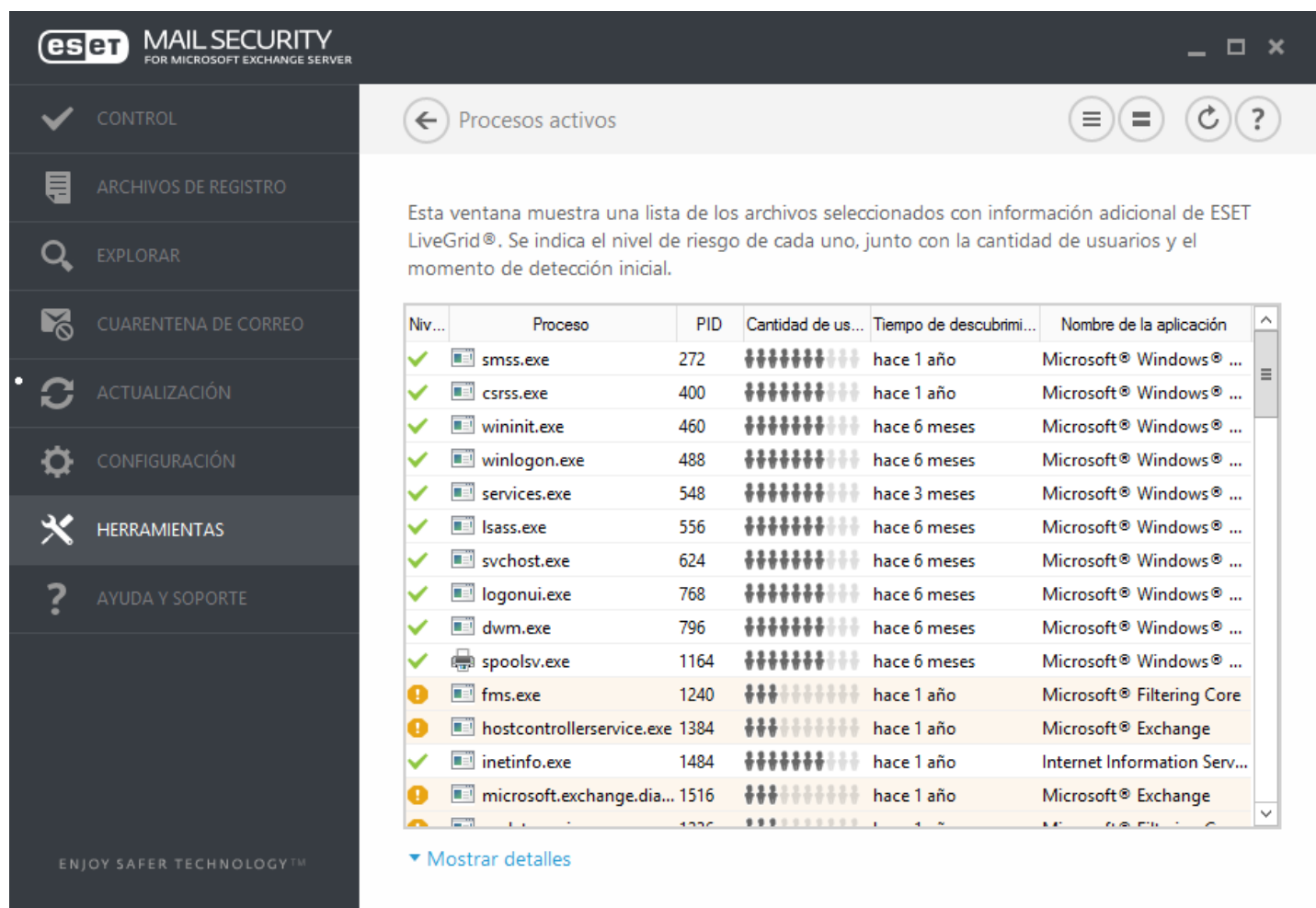
El menú Herramientas incluye módulos que ayudan a simplificar la administración del programa y ofrecen opciones adicionales. Incluye las siguientes herramientas:

- [Procesos activos](#)
- [Observar la actividad](#)
- [Estadísticas de la protección](#)
- [Cluster](#)
- [Shell de ESET](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#)
- [Tareas programadas](#)
- [Enviar el archivo para su análisis](#)
- [Cuarentena](#)



3.7.1 Procesos activos

Los procesos activos muestran los programas o procesos activos en su equipo y mantiene a ESET informado de manera instantánea y continua sobre las nuevas infiltraciones. ESET Mail Security proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología <%ELG%> habilitada.



Esta ventana muestra una lista de los archivos seleccionados con información adicional de ESET LiveGrid®. Se indica el nivel de riesgo de cada uno, junto con la cantidad de usuarios y el momento de detección inicial.

Niv...	Proceso	PID	Cantidad de us...	Tiempo de descubrimi...	Nombre de la aplicación
✓	smss.exe	272	██████████	hace 1 año	Microsoft® Windows® ...
✓	csrss.exe	400	██████████	hace 1 año	Microsoft® Windows® ...
✓	wininit.exe	460	██████████	hace 6 meses	Microsoft® Windows® ...
✓	winlogon.exe	488	██████████	hace 6 meses	Microsoft® Windows® ...
✓	services.exe	548	██████████	hace 3 meses	Microsoft® Windows® ...
✓	lsass.exe	556	██████████	hace 6 meses	Microsoft® Windows® ...
✓	svchost.exe	624	██████████	hace 6 meses	Microsoft® Windows® ...
✓	logonui.exe	768	██████████	hace 6 meses	Microsoft® Windows® ...
✓	dwm.exe	796	██████████	hace 6 meses	Microsoft® Windows® ...
✓	spoolsv.exe	1164	██████████	hace 6 meses	Microsoft® Windows® ...
!	fms.exe	1240	██████████	hace 1 año	Microsoft® Filtering Core
!	hostcontroller.service.exe	1384	██████████	hace 1 año	Microsoft® Exchange
✓	inetinfo.exe	1484	██████████	hace 1 año	Internet Information Serv...
!	microsoft.exchange.dia...	1516	██████████	hace 1 año	Microsoft® Exchange

Mostrar detalles

Nivel de riesgo: en la mayoría de los casos, la tecnología ESET Mail Security y <%ELG%> les asigna niveles de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, usa una serie de reglas heurísticas que examinan las características de cada objeto y después estima su potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asigna un nivel de riesgo desde el valor **1: seguro (en color verde)** hasta **9: peligroso (en color rojo)**.

Proceso: el nombre de la imagen del programa o proceso que se está ejecutando actualmente en el equipo. También puede usar el Administrador de tareas de Windows para ver todos los procesos activos en el equipo. Puede abrir el Administrador de tareas al hacer clic con el botón secundario en un área vacía de la barra de tareas seleccionado, posteriormente, el Administrador de tareas, o al presionar **Ctrl+Shift+Esc** en su teclado.

PID: es un identificador de procesos activos en los sistemas operativos de Windows.

i NOTA

Las aplicaciones conocidas marcadas como **Seguras (en verde)** indudablemente no están infectadas (figuran en la lista blanca) y se excluyen de la exploración, ya que de esta forma se mejora la velocidad de exploración correspondiente a la exploración del equipo a petición o la protección del sistema de archivos en tiempo real en el equipo.

Cantidad de usuarios: la cantidad de usuarios que usan una aplicación específica. Estos datos se recopilan con la tecnología <%ELG%>.

Momento de detección: periodo transcurrido desde que la tecnología <%ELG%> descubrió la aplicación.

i NOTA

Cuando una aplicación se marca como **Desconocida (naranja)**, quizá no sea necesariamente un software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, use la función [Enviar el muestra para su análisis](#) para enviar el archivo al laboratorio de virus de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección en una de las próximas actualizaciones de la base de datos de firmas de virus.

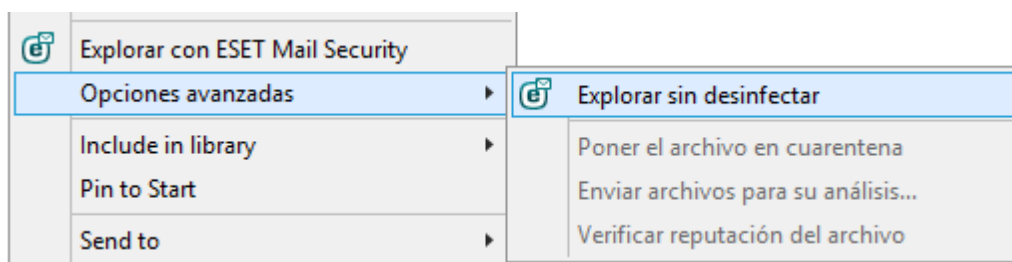
Nombre de aplicación: nombre determinado de un programa al cual pertenece este proceso.

Al hacer clic en una aplicación determinada que se encuentra abajo, aparecerá la siguiente información en el sector inferior de la ventana:

- **Ruta:** ubicación de una aplicación en su equipo.
- **Tamaño:** tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Descripción:** características del archivo según la descripción proporcionada por el sistema operativo.
- **Empresa:** nombre del proveedor o del proceso de la aplicación.
- **Versión:** información proporcionada por el desarrollador de la aplicación.
- **Producto:** nombre de la aplicación y/o nombre comercial.
- **Creada el:** fecha y hora de la creación de una aplicación.
- **Modificada el:** última fecha y hora en que se modificó una aplicación.

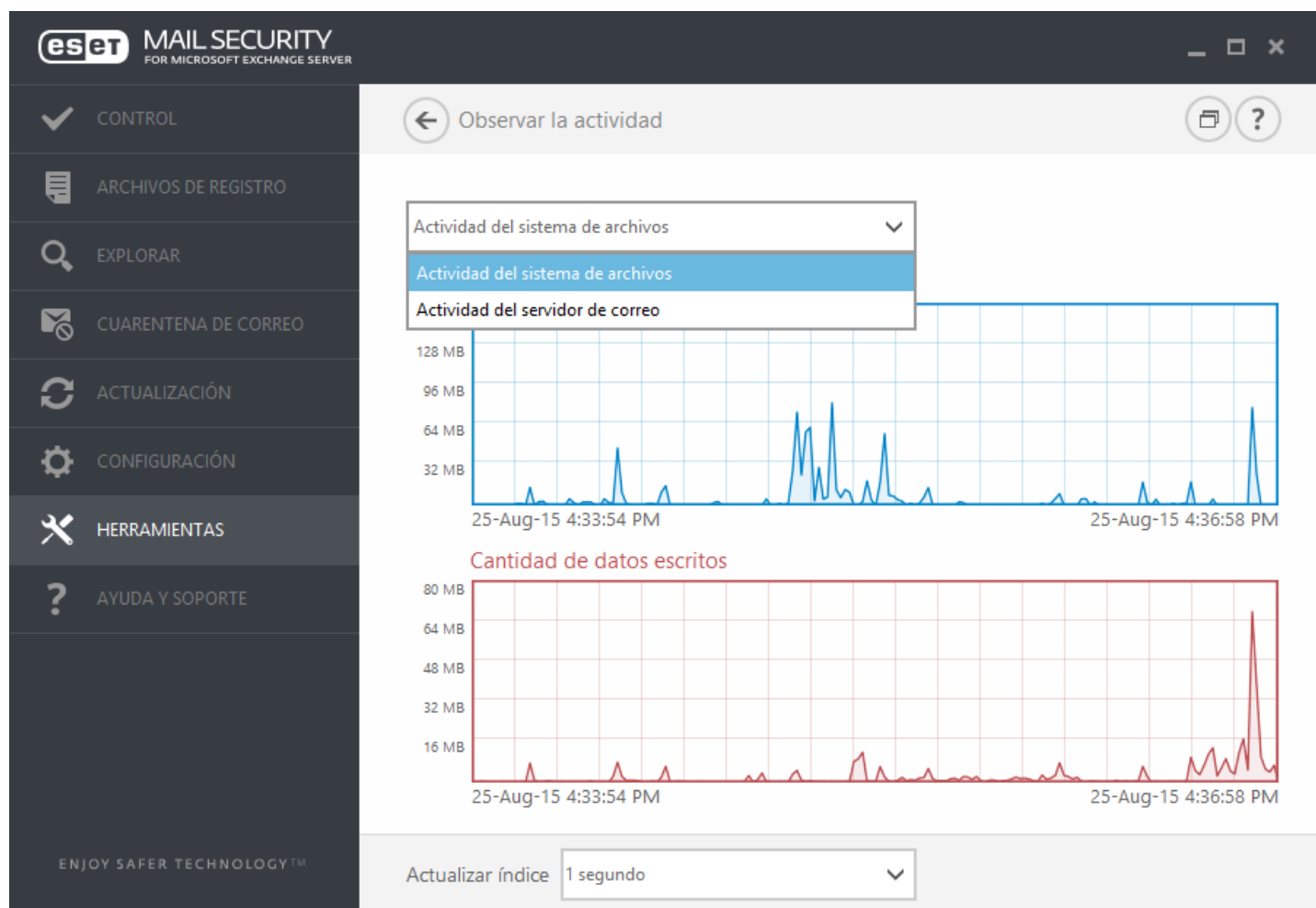
i NOTA

También se puede revisar la reputación de archivos que no sean programas o procesos - para ello, marque los archivos que desea verificar, haga un clic con el botón derecho en ellos y seleccione **Opciones avanzadas > Verificar la reputación de archivos mediante <%ELG%>** del [menú contextual](#).



3.7.2 Observar la actividad

Para ver la **Actividad del sistema de archivos** actual y la **Actividad del servidor de correo** en forma de gráfico, haga clic en **Herramientas > Observar actividad**. En el sector inferior del gráfico hay una línea de tiempo que registra la actividad del sistema de archivos en tiempo real conforme al intervalo de tiempo seleccionado. Use el menú desplegable de **Frecuencia de actualización** para cambiar la frecuencia de las actualizaciones.



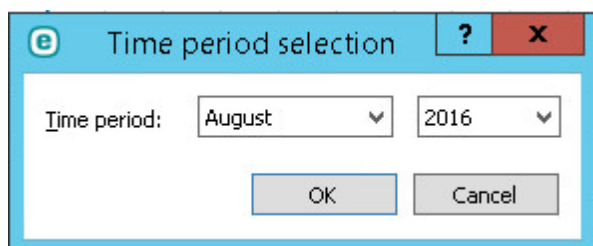
Se encuentran disponibles las siguientes opciones:

- **1 segundo** : el gráfico se actualiza cada segundo y la línea de tiempo abarca los últimos 10 minutos.
- **1 minuto (últimas 24 horas)** : el gráfico se actualiza cada minuto y la línea de tiempo abarca las últimas 24 horas.
- **1 hora (último mes)** : el gráfico se actualiza cada hora y la línea de tiempo abarca el último mes.
- **1 hora (mes seleccionado)** : el gráfico se actualiza cada hora y la línea de tiempo abarca el mes seleccionado. Haga clic en el botón **Cambiar mes** para realizar otra selección.

El eje vertical del **Gráfico de** actividad del sistema de archivos representa la cantidad de datos leídos (en azul) y la cantidad de datos escritos (en rojo). Ambos valores están representados en kB (kilobytes)/MB/GB. Al pasar el mouse sobre los datos leídos o escritos en la leyenda que se encuentra abajo del gráfico, el gráfico solo mostrará los datos correspondientes a ese tipo de actividad.

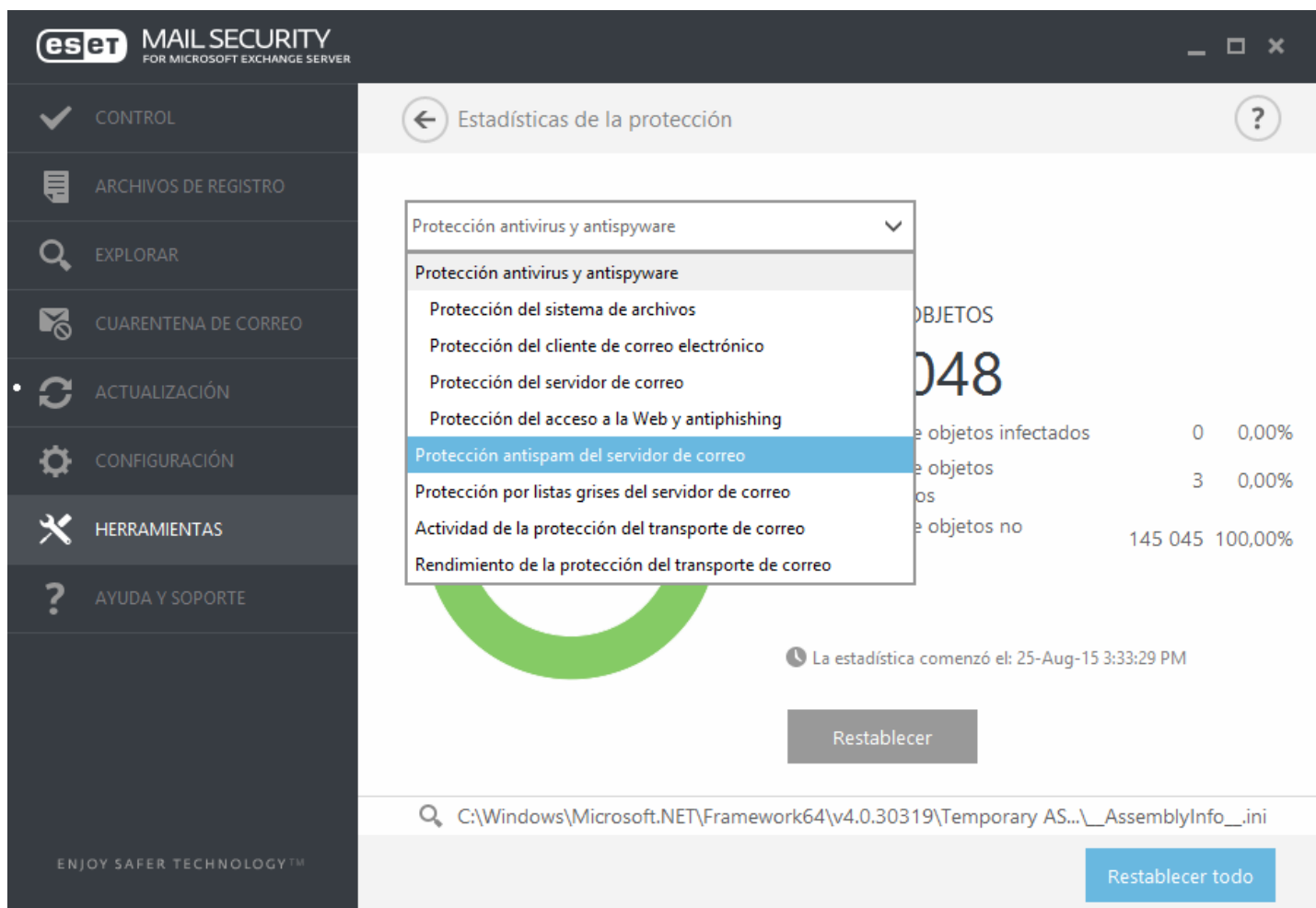
3.7.2.1 Selección del período de tiempo

Seleccione un mes (y un año) para el que desee visualizar la **Actividad del sistema de archivos** o **Actividad del servidor de correo** en el gráfico.



3.7.3 Estadísticas de la protección

Para ver un gráfico de datos estadísticos relacionados con los módulos de protección de ESET Mail Security, haga clic en **Herramientas > Estadísticas de la protección**. Seleccione el módulo de protección deseado del menú desplegable para ver el gráfico y la leyenda correspondientes. Pase el mouse sobre un elemento de la leyenda para mostrar los datos de ese elemento en el gráfico.



Están disponibles los siguientes gráficos de estadísticas:

- **Protección antivirus y antispyware:** muestra la cantidad general de objetos infectados y desinfectados.
- **Protección del sistema de archivos:** solo muestra los objetos que fueron leídos o escritos en el sistema de archivos.
- **Protección del cliente de correo electrónico:** muestra los objetos que fueron enviados o recibidos por clientes de correo electrónico únicamente.
- **Protección del servidor de correo:** muestra las estadísticas antivirus y antispyware del servidor de correo.
- **Acceso web y protección antiphishing:** muestra los objetos descargados por los navegadores web únicamente.
- **Protección antispam del servidor de correo:** muestra las estadísticas históricas del antispam desde el último inicio del sistema.
- **Protección por listas grises del servidor de correo:** incluye las estadísticas antispam generadas por el método de creación de listas grises.
- **Actividad de la protección del transporte de correo:** muestra los objetos verificados, bloqueados y eliminados por el servidor de correo.
- **Rendimiento de la protección del transporte de correo:** muestra los datos procesados por VSAPI/Agente de transporte en B/s.
- **Actividad de protección de la base de datos de la casilla de correo:** muestra los objetos procesados por VSAPI (cantidad de **objetos verificados, en cuarentena y eliminados**).
- **Rendimiento de la protección de la base de datos de la casilla de correo:** muestra la información procesada por VSAPI (cantidad de promedios distintos para **Hoy**, para los **Últimos 7 días** y los promedios **Desde el último reinicio**).

Junto a los gráficos de estadísticas, puede ver la cantidad total de objetos explorados, infectados, desinfectados y no infectados. Haga clic en **Restablecer** para borrar toda la información estadística o haga clic en **Restablecer todo** para borrar y quitar todos los datos existentes.

3.7.4 Cluster

El **Cluster de ESET** es una infraestructura de comunicación P2P de la línea de productos ESET para Microsoft Windows Server.

Esta infraestructura habilita los productos del servidor de ESET para que se comuniquen entre los mismos e intercambien los datos como la configuración y las notificaciones. y puede [Sincronizar las bases de datos de la lista gris](#) además de sincronizar los datos necesarios para un funcionamiento correcto de un grupo de instancias de productos. Un ejemplo de dichos grupos es un grupo de nodos en un Cluster de Windows Failover o Equilibrio de carga de la red (NLB) con un producto ESET instalado donde sea necesario contar con la misma configuración del producto a lo largo de todo el clúster. Los Clusteres de ESET aseguran esta consistencia entre las instancias.

i NOTA

La configuración de la [interfaz de usuario](#) no se sincroniza entre los nodos del clúster de ESET.

Se puede acceder a la página de estado de los clústeres de ESET desde el menú principal en **Herramientas > Cluster** si se encuentra bien configurada, la página de estado debería verse de la siguiente manera:

The screenshot shows the ESET Mail Security for Microsoft Exchange Server interface. On the left is a dark sidebar with a menu containing: MONITORING (checked), LOG FILES, SCAN, MAIL QUARANTINE, UPDATE, SETUP, TOOLS, and HELP AND SUPPORT. The main area has a header with a back arrow, the word 'Cluster', and refresh/help icons. Below this is a table with two columns: 'Name' and 'State'. The table lists four nodes, all with a state of 'Online'. At the bottom of the main area are three buttons: 'Cluster wizard...', 'Import certificates...', and 'Destroy cluster'.

Name	State
WIN-JDLB8CEUR5	Online
W2012R2-NODE1	Online
W2012R2-NODE2	Online
W2012R2-NODE3	Online

Para configurar el Cluster de ESET haga clic en **Asistente de clúster...** Para obtener más detalles sobre cómo configurar el clúster de ESET con el asistente, haga clic [aquí](#).

Al configurar el Cluster de ESET, hay dos formas de agregar nodos: en forma automática con un clúster de Windows Failover/NLB existente, o en forma manual buscando los equipos que se encuentren en un grupo de trabajo o en un dominio.

Autodetectar: detecta automáticamente los nodos que ya son parte de clústeres de Windows Failover/NLB y los agrega al clúster de ESET.

Examinar: para agregar los nodos en forma manual, ingrese los nombres de servidor (ya sean miembros del mismo grupo de trabajo o del mismo dominio).

i NOTA

los servidores no tienen que ser miembros de un clúster de Windows Failover/NLB para usar la función del clúster de ESET. No necesita un clúster de Windows Failover o NLB en su entorno para usar los clústeres de ESET.

Una vez que haya agregado los nodos a su clúster de ESET, el siguiente paso es la instalación de ESET Mail Security en cada uno de ellos. Esto se hace en forma automática durante la configuración del clúster de ESET.

Credenciales necesarias para la instalación remota de ESET Mail Security en otros nodos de clúster:

- **Escenario de dominio:** credenciales del administrador de dominios
- **Escenario de un grupo de trabajo:** debe asegurarse de que todos los nodos usen las mismas credenciales de la cuenta del administrador local

En un clúster de ESET, también puede usar una combinación de nodos agregados en forma automática como parte de los clústeres de Windows Failover/NLB existentes y los nodos agregados en forma manual (siempre que se encuentren dentro del mismo dominio).

i NOTA

No es posible combinar los nodos de dominio con los nodos de grupos de trabajo.

Otro requisito para el uso de un clúster de ESET es que la función **Compartir archivos e impresoras** debe encontrarse habilitada dentro del Firewall de Windows antes de forzar la instalación de ESET Mail Security en los nodos del clúster de ESET.

Es fácil desarmar los clústeres de ESET con un clic en **Destruir clúster**. Cada nodo escribirá un informe en su registro de eventos sobre la destrucción del clúster de ESET. Luego, todas las reglas del firewall de ESET se eliminan del Firewall de Windows. Los nodos anteriores vuelven a su estado anterior y pueden volver a usarse en otro clúster de ESET, de ser necesario.

i NOTA

la creación de los clústeres de ESET entre ESET Mail Security y Seguridad de archivos de ESET para Linux no son compatibles.

Agregar los nuevos nodos a un clúster de ESET puede llevarse a cabo en cualquier momento a través del **Asistente de clúster** de la misma forma en la que se describió anteriormente y [aquí](#).

3.7.4.1 Asistente de clúster: página 1

El primer paso al configurar un clúster de ESET es agregar los nodos. Para agregar los nodos, puede usar la opción **Autodetectar** o **Explorar**. Asimismo, puede ingresar el nombre del servidor dentro del cuadro de texto y hacer clic en **Agregar**.

Autodetectar agrega en forma automática los nodos desde un clúster de Windows Failover Cluster/Network Load Balancing (NLB). Para poder agregar los nodos en forma automática, es necesario que el servidor que usa para crear el clúster de ESET sea parte de este clúster de Windows Failover/NLB. El clúster NLB debe tener habilitada la opción **Permitir control remoto** en las propiedades de clúster para que el Cluster de ESET pueda detectar los nodos en forma correcta. Una vez que tenga la lista de los nodos agregados recientemente, puede quitar los que no desea.

Haga clic en **Examinar** para buscar y seleccionar los equipos dentro de un dominio o un grupo de trabajo. Este método permite agregar los nodos al clúster de ESET de forma manual. Otra forma de agregar los nodos es escribir el nombre del host del servidor que desea agregar y hacer clic en **Agregar**.

Select nodes

?

Machine to add to the list of cluster nodes

Cluster nodes

W2012R2-NODE1
W2012R2-NODE2
W2012R2-NODE3
WIN-JDLB8CEUR5

Add

Remove

Remove all

Autodetect

Browse...

Next >

Cancel

Para modificar los **Nodos de clúster** en el listado, seleccione el clúster que desea quitar y haga clic en **Eliminar**, o para vaciar la lista completa, haga clic en **Eliminar todos**.

Si ya cuenta con un clúster de ESET, puede agregarle los nodos nuevos en cualquier momento. Los pasos a seguir son los mismos.

i NOTA

todos los nodos que se mantienen en el listado deben encontrarse en línea y ser accesibles. Por defecto, el host local se agrega a los nodos de clúster.

3.7.4.2 Asistente de clúster: página 2

Defina el nombre de clúster, el modo de distribución del certificado y si se instala el producto en los otros nodos o no.

Cluster name and install type

?

Cluster name

clusterName

Listening port

9777

☒ Open port in Windows firewall

Certificate distribution

☒ Automatic remote

☐ Manual

Generate...

Product installation on other nodes

☒ Automatic remote

☐ Manual

☒ Push license to nodes without activated product

< Previous

Next >

Cancel

Nombre del clúster: ingrese el nombre del clúster.

Puerto de escucha (el puerto predeterminado es 9777)

Puerto abierto en el firewall de Windows: cuando se selecciona, se crea una regla en el Firewall de Windows.

Distribución de certificados:

Remoto automático: el certificado se instalará en forma automática.

Manual: al hacer clic en **Generar**, se abre una ventana de exploración; seleccione la carpeta en donde almacenar los certificados. Se creará un certificado de raíz al igual que un certificado por cada nodo, incluido el que se usa (máquina local) para configurar el clúster de ESET. Puede elegir inscribir el certificado en la máquina local al hacer clic en **Sí**. Necesitará importar los certificados en forma manual, como se explica [aquí](#).

Instalación del producto a otros nodos:

Remoto automático: ESET Mail Security se instalará automáticamente en cada nodo (siempre y cuando los sistemas operativos sean de la misma arquitectura).

Manual: seleccione esta opción si desea instalar ESET Mail Security en forma manual (por ejemplo, cuando cuenta con diferentes arquitecturas de los sistemas operativos en algunos de los nodos).

Insertar la licencia en los nodos con el producto desactivado: seleccione esta opción para que ESET Security active automáticamente ESET Solutions instalada en los nodos sin licencias.

i NOTA

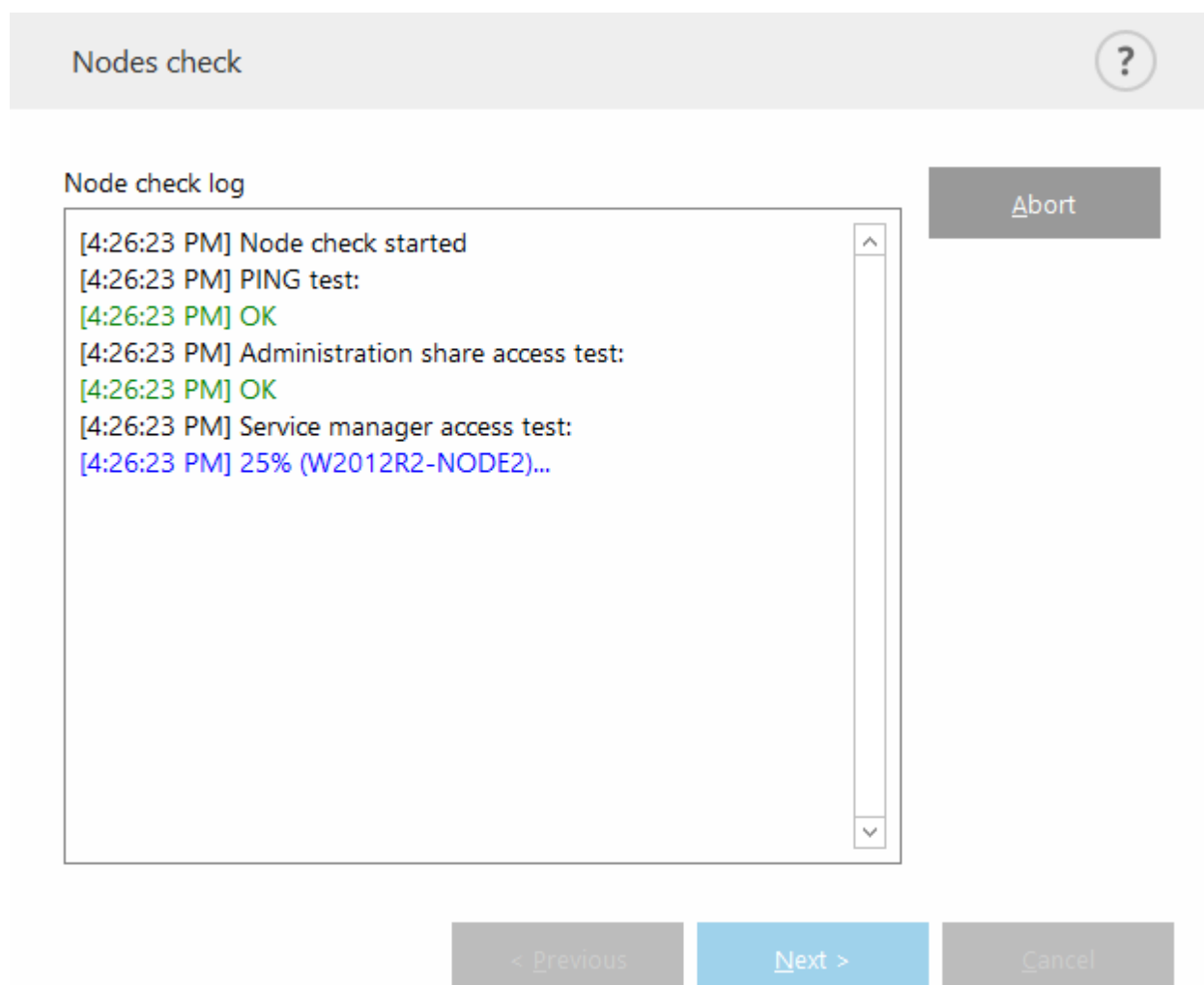
si desea crear un Cluster de ESET con las arquitecturas de los sistemas operativos mixtos (32 y 64 bits), tendrá que instalar ESET Mail Security en forma manual. Los sistemas de operación en uso se detectarán en los pasos

siguientes y verá esta información en la ventana de registro.

3.7.4.3 Asistente de clúster: página 3

Luego de especificar los detalles de la instalación, se lleva a cabo una verificación del nodo. Verá las siguientes comprobaciones en el **Registro de verificación de nodos**:

- verifique que todos los nodos existentes se encuentren en línea
- verifique que se pueda acceder a todos los nodos
- el nodo se encuentra en línea
- se puede acceder a la porción de administrador
- es posible la ejecución remota
- las versiones de producto correctas (o sin producto) se instalaron.
- verifique que los nuevos certificados estén presentes



Verá el informe una vez que finalice la verificación del nodo:

Nodes check

?

Node check log

[4:37:36 PM] Node check started
[4:37:36 PM] PING test:
[4:37:36 PM] OK
[4:37:36 PM] Administration share access test:
[4:37:37 PM] OK
[4:37:37 PM] Service manager access test:
[4:38:22 PM] OK
[4:38:22 PM] Checking installed product version and features:
[4:38:22 PM] W2012R2-NODE1: Install will be performed.
[4:38:22 PM] W2012R2-NODE2: Install will be performed.
[4:38:22 PM] W2012R2-NODE3: Install will be performed.
[4:38:24 PM] OK

Check

< Previous

Next >

Cancel

3.7.4.4 Asistente de clúster: página 4

Cuando sea necesario instalar el producto en un equipo remoto durante el arranque del clúster de ESET, el paquete de instalación verifica el directorio %ProgramData%\ESET\<Produt_name>\Installer en busca de la presencia del instalador. Si no se encuentra el paquete del instalador en esa ubicación, se le solicita al usuario que ubique uno.

Nodes install and cluster activation

Product install log

Press the Install button to begin the cluster install process.

Install

< Previous

Finish

Cancel

i NOTA

al intentar usar la instalación remota automática para un nodo con una arquitectura diferente (32 bit vs 64 bit), se detectará y se recomendará realizar una instalación manual.

i NOTA

si instaló una versión anterior de ESET Mail Security en algunos nodos, debe reinstalar ESET Mail Security con una versión más reciente en estos equipos antes de crear el clúster. Esto puede producir un reinicio automático en esos equipos. Si esto sucede, verá una señal de advertencia.

Product install log

[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.


Install

< Previous

Finish

Cancel

Una vez que haya configurado el clúster de ESET en forma correcta, aparecerá como habilitado en la página **Configuración > Servidor**.

MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

✓MONITORING

LOG FILES

SCAN

MAIL QUARANTINE

UPDATE

SETUP

TOOLS

HELP AND SUPPORT

ENJOY SAFER TECHNOLOGY™

Setup

Server

Computer

Tools

Automatic exclusions

Enabled

Cluster

Enabled

Antivirus protection

Enabled

Antispam protection

Enabled

Import/Export settings

Advanced setup

Asimismo, puede verificar su estado actual en la página de estado del clúster (**Herramientas > clúster**).

The screenshot shows the ESET Mail Security for Microsoft Exchange Server interface. On the left is a dark sidebar with navigation options: MONITORING (checked), LOG FILES, SCAN, MAIL QUARANTINE, UPDATE, SETUP, TOOLS, and HELP AND SUPPORT. The main area is titled 'Cluster' and contains a table with the following data:

Name	State
WIN-JDLB8CEUR5	Online
W2012R2-NODE1	Online
W2012R2-NODE2	Online
W2012R2-NODE3	Online

Below the table are three buttons: 'Cluster wizard...', 'Import certificates...', and 'Destroy cluster'. The bottom of the sidebar features the text 'ENJOY SAFER TECHNOLOGY™'.

Importar certificados: navegue a la carpeta que contiene los certificados (generados durante el uso del [Asistente del clúster](#)). Seleccione el archivo del certificado y haga clic en **Abrir**.

3.7.5 Shell de ESET

eShell (abreviación de Shell de ESET) es una interfaz de línea de comandos para ESET Mail Security. Es una alternativa a la interfaz gráfica de usuario (GUI). eShell cuenta con todas las características y opciones que la GUI normalmente le brinda. eShell permite configurar y administrar el programa completo sin necesidad de usar la GUI.

Además de todas las funciones y funcionalidades disponibles en la GUI, también ofrece la opción de automatizar tareas mediante la ejecución de scripts para configurar, modificar la configuración o realizar una acción. Asimismo, eShell puede resultar útil para quienes prefieren usar la línea de comandos en lugar de la GUI.

eShell se puede ejecutar en dos modos:

- **Modo interactivo:** es útil cuando desea trabajar con eShell (no solamente ejecutar un único comando), por ejemplo, para aquellas tareas como cambiar la configuración, visualizar registros, etc. Puede usar el modo interactivo si aún no se familiarizó aún con los comandos. El modo interactivo hace que el desplazamiento por eShell sea más sencillo. Además, muestra los comandos disponibles que puede usar dentro de un contexto determinado.
- **Comando simple/modo de procesamiento por lotes:** puede usar este modo si solamente necesita ingresar un comando sin ingresar al modo interactivo de eShell. Esto puede realizarlo desde el Símbolo de sistema de Windows al escribir en `eshell` con los parámetros apropiados. Por ejemplo:

```
eshell get status Oeshell set antivirus status disabled
```

Para ejecutar ciertos comandos (como el segundo ejemplo anterior) en modo de procesamiento por lotes/script, primero debe [configurar](#) una serie de configuraciones. De lo contrario, verá un mensaje de **Acceso denegado**. Esto es por razones de seguridad.

i NOTA

para la funcionalidad completa, le recomendamos abrir eShell con **Ejecutar como administrador**. Lo mismo aplica al ejecutar un único comando a través del Símbolo del sistema de Windows (cmd). Abra el símbolo con **Ejecutar como administrador**. De lo contrario, no podrá ejecutar todos los comandos. Si no puede ejecutar el símbolo del sistema como Administrador, no se le permitirá ejecutar los comandos debido a la falta de permisos.

i NOTA

para ejecutar los comandos de eShell desde el Símbolo de comandos de Windows o para ejecutar archivos de procesamiento por lotes, debe realizar algunas configuraciones. Para obtener más información acerca de cómo ejecutar archivos por lotes, haga clic [aquí](#).

Para ingresar al modo interactivo en eShell, puede usar una de los siguientes dos métodos:

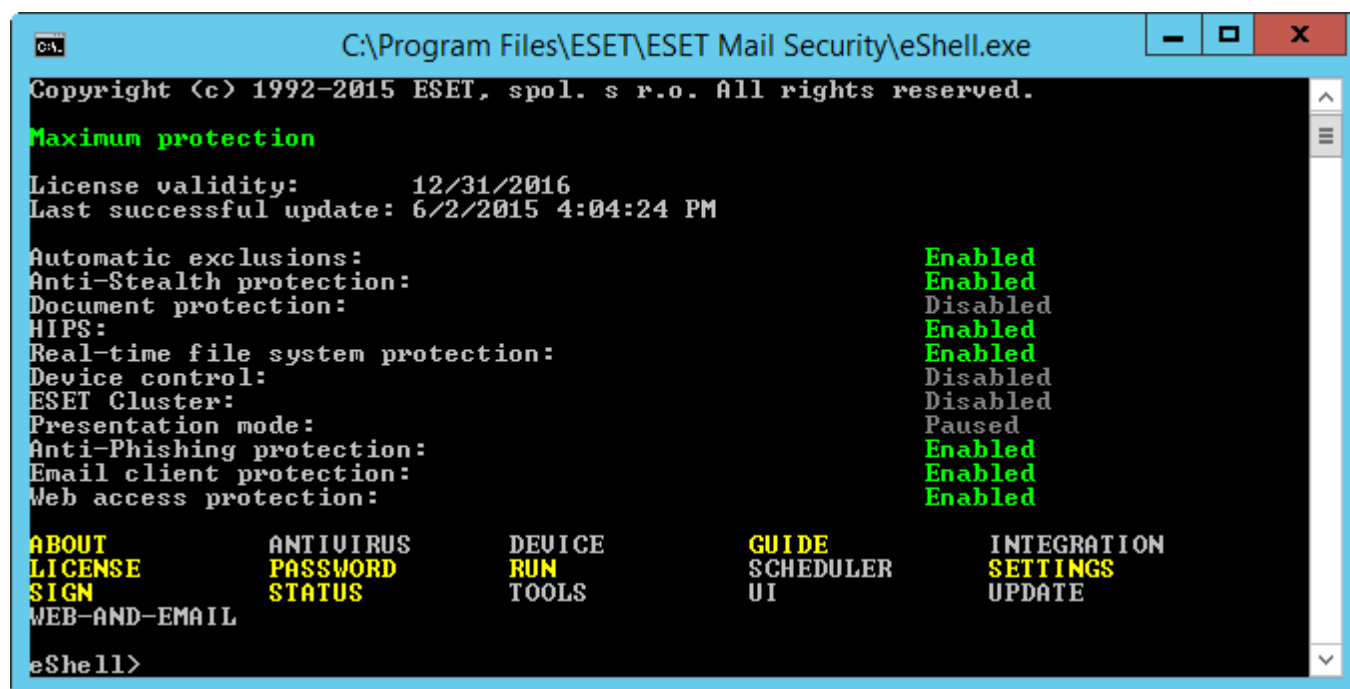
- Desde el menú de inicio de Windows: **Inicio > Todos los programas > ESET > ESET Mail Security > Shell de ESET**
- Desde Símbolo del sistema de Windows, tras escribir `eshell` y presionar la tecla **Intro**

Al ejecutar eShell en modo interactivo por primera vez, se mostrará la pantalla de primera vista (guía).

i NOTA

si en el futuro desea mostrar la pantalla de primera vista, escriba el comando `guide`. Muestra algunos ejemplos básicos sobre cómo usar eShell con Sintaxis, Prefijo, Ruta del comando, Formas abreviadas, Alias, etc. Básicamente, consiste en una guía rápida para usar eShell.

La próxima vez que ejecute eShell, verá esta pantalla:



```
C:\Program Files\ESET\ESET Mail Security\eShell.exe
Copyright (c) 1992-2015 ESET, spol. s r.o. All rights reserved.
Maximum protection
License validity:      12/31/2016
Last successful update: 6/2/2015 4:04:24 PM
Automatic exclusions: Enabled
Anti-Stealth protection: Enabled
Document protection: Disabled
HIPS: Enabled
Real-time file system protection: Enabled
Device control: Disabled
ESET Cluster: Disabled
Presentation mode: Paused
Anti-Phishing protection: Enabled
Email client protection: Enabled
Web access protection: Enabled
ABOUT      ANTI VIRUS    DEVICE      GUIDE      INTEGRATION
LICENSE     PASSWORD     RUN         SCHEDULER  SETTINGS
SIGN        STATUS      TOOLS      UI          UPDATE
WEB-AND-EMAIL
eShell>
```

i NOTA

los comandos no diferencian entre mayúsculas de minúsculas. Puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Personalización de eShell

Puede personalizar eShell en contexto `ui eshell`. Puede configurar alias, colores, idiomas, políticas de ejecución para [scripts](#); puede elegir mostrar comandos ocultos y otras configuraciones.

3.7.5.1 Uso

Sintaxis

Los comandos deben formatearse con la sintaxis correcta para que funcionen y pueden estar compuesto por prefijos, contextos, argumentos, opciones, etc. Esta es la sintaxis general que se usa en eShell:

[<prefijo>] [<ruta del comando>] <comando> [<argumentos>]

Ejemplo (para activar la protección de documentos):

CONFIGURAR EL ESTADO DEL DOCUMENTO ANTIVIRUS HABILITADO

SET : un prefijo

DOCUMENTO ANTIVIRUS : ruta a un comando en particular, un contexto al cual pertenece dicho comando

ESTADO : el comando en sí

ENABLED : un argumento para el comando

Al usar ? como un argumento para el comando, se mostrará la sintaxis para ese comando específico. Por ejemplo, STATUS ? le mostrará la sintaxis del comando STATUS:

SINTAXIS:

[get] | status

set status enabled | disabled

Como puede ver, [get] está entre paréntesis. Esto indica que el prefijo get es el valor predeterminado del comando status. Significa que, al ejecutar estado sin especificar ningún prefijo, usará, de hecho, el prefijo predeterminado (en este caso, get status). El uso de comandos sin prefijo ahorra tiempo de escritura. Generalmente, get es el prefijo predeterminado para la mayoría de los comandos, pero debe asegurarse cuál es el predeterminado para un comando en particular y que es exactamente lo que usted desea ejecutar.

i NOTA

los comandos no distinguen mayúsculas de minúsculas; puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Prefijo/operación

Un prefijo es una operación. El prefijo GET le dará información acerca de cómo está configurada una característica determinada de ESET Mail Security, o le mostrará un estado (OBTENER ESTADO DEL ANTIVIRUS le mostrará el estado actual de protección). El prefijo SET configurará la funcionalidad o cambiará su estado (CONFIGURAR EL ESTADO DEL ANTIVIRUS HABILITADO activará la protección).

Estos son los prefijos que eShell le permite usar. Un comando puede soportar, o no, alguno de los siguientes prefijos:

GET : devuelve la configuración o el estado actual

SET : establece el valor o el estado

SELECT : selecciona un elemento

ADD : agrega un elemento

REMOVE : quita un elemento

CLEAR : borra todos los elementos o archivos

START : inicia una acción

STOP : detiene una acción

PAUSE : pone una acción en pausa

RESUME : reanuda una acción

RESTORE : restaura la configuración predeterminada, el objeto o el archivo

SEND : envía un objeto o un archivo

IMPORT : importa desde un archivo

EXPORT : exporta a un archivo

Los prefijos como GET y SET se usan con muchos comandos; pero algunos comandos (como EXIT) no usan prefijos.

Ruta del comando/contexto

Los comandos se ubican en contextos que conforman una estructura con forma de árbol. El nivel superior del árbol es “root”. Cuando ejecuta eShell, está en el nivel root:

```
eShell>
```

Puede ejecutar un comando desde allí o ingresar el nombre del contexto para navegar dentro del árbol. Por ejemplo, al ingresar el contexto `HERRAMIENTAS`, mostrará una lista de todos los comandos y subcontextos que están disponibles desde ese nivel.



Los elementos amarillos son los comandos que se pueden ejecutar y los grises son los subcontextos que se pueden ingresar. Un subcontexto contiene más comandos.

Si necesita volver a un nivel superior, use `..` (dos puntos seguidos). Por ejemplo, si usted se encuentra aquí:

```
inicio del> antivirus eShell
```

escriba `..` y lo llevará a un nivel superior, es decir, a:

```
eShell antivirus>
```

Si desea volver a root desde `inicio del> antivirus eShell` (que está dos niveles más abajo que la raíz), simplemente escriba `.. ..` (dos puntos seguidos y dos puntos seguidos separados por un espacio). De esta manera, subirá dos niveles, que en este caso es root. Use una barra diagonal inversa `\` para regresar directamente a la raíz desde cualquier nivel, independientemente de la profundidad del árbol del contexto en la que se encuentre. Si desea ir a un contexto específico en niveles superiores, solo use el número adecuado de `..` como sea necesario para ir al nivel deseado, use espacio como separador. Por ejemplo, si desea ir tres niveles más arriba, use `.. .. .`

La ruta es relativa al contexto actual. Si el comando está incluido en el contexto actual, no ingrese una ruta. Por ejemplo, para ejecutar `OBTENER ESTADO DEL ANTIVIRUS` ingrese:

```
OBTENER ESTADO DEL ANTIVIRUS : si usted está en el nivel root (la línea de comandos muestra eShell>)
GET STATUS : si usted está en el contexto ANTIVIRUS (la línea de comandos muestra eShell antivirus>)
.. GET STATUS : si usted está en el contexto INICIO DEL ANTIVIRUS (la línea de comandos muestra inicio del>
antivirus eShell)
```

NOTA

puede usar un solo `.` (punto) en vez de dos `..` porque un solo punto es una abreviatura de los dos puntos. Por ejemplo:

```
. GET STATUS : si usted está en el contexto INICIO DEL ANTIVIRUS (la línea de comandos muestra inicio del>
antivirus eShell)
```

Argumento

Un argumento es una acción que se realiza para un comando en particular. Por ejemplo, el comando `NIVEL DESINFECTADO` (ubicado en `MOTOR EN TIEMPO REAL DEL ANTIVIRUS`) puede usarse con los siguientes argumentos:

`no` - Sin desinfección
`normal` - Desinfección normal
`strict` : desinfección estricta

Otro ejemplo son los argumentos `ENABLED` o `DISABLED`, que se usan para habilitar o deshabilitar cierta característica o funcionalidad.

Forma simplificada/comandos abreviados

eShell permite abreviar los contextos, los comandos y los argumentos (siempre y cuando el argumento sea un modificador o una opción alternativa). No es posible abreviar un prefijo o un argumento que sea un valor concreto, como un número, un nombre o una ruta.

¡ NOTA

Puede usar números `1` y `0` en lugar de argumentos `shabilitados` y `deshabilitados`. Por ejemplo:

```
set status enabled => set stat 1
set status disabled => set stat 0
```

Ejemplos de la forma abreviada:

```
set status enabled => set stat en
agregar explorador de antivirus común, excluye C:\path\file.ext => agregar exploración antivirus común C:\pa
```

En caso de que dos comandos o contextos comiencen con las mismas letras (por ejemplo, `ABOUT` y `ANTIVIRUS`, y usted escribe `A` como un comando abreviado), eShell no podrá decidir cuál de estos dos comandos desea ejecutar.

Aparecerá un mensaje de error y la lista de los comandos que comienzan con “A”, desde donde usted podrá elegir uno:

```
eShell>a
El siguiente comando no es único: a
```

Los siguientes comandos están disponibles en este contexto:

```
ABOUT: muestra información sobre el programa
ANTIVIRUS: cambia a antivirus contextual
```

Al agregar una o más letras (por ej., `AB` en lugar de solamente `A`) eShell ejecutará el comando `ABOUT`, ya que ahora es único.

¡ NOTA

para estar seguro de que el comando se ejecute como lo necesita, es recomendable no abreviar los comandos, los argumentos, etc. y usar la forma completa. De esta manera, se ejecutará exactamente como usted lo requiere y se evitarán errores no deseados. Es recomendable en particular para archivos o scripts de procesamiento por lotes.

Finalización automática

Es una nueva función de eShell desde la versión 2.0. Es muy similar a la finalización automática del Símbolo de comandos de Windows. Mientras que Símbolo del sistema de Windows completa rutas de archivos, eShell completa comandos, nombres de contextos y operaciones. No es compatible con la finalización de argumentos. Al escribir un comando solo presione la tecla `TAB` para completar o recorrer el ciclo de variaciones disponibles. Presione **SHIFT + TAB** para retroceder en el ciclo. No es compatible con la combinación de forma abreviada y finalización automática. Use una de las dos. Por ejemplo, al escribir `exploración antivirus en tiempo real` presionar la tecla `TAB` no hará nada. En vez de eso, escriba `antivirus` y luego presione `TAB` para completar el `antivirus`, prosiga escribiendo en tiempo real + `TAB` y exploración + `TAB`. Entonces podrá recorrer el ciclo con todas las variaciones disponibles: crear-exploración, ejecutar-exploración, abrir-exploración, etc.

Alias

Un alias es un nombre alternativo que se puede usar para ejecutar un comando (siempre y cuando el comando tenga un alias asignado). Hay algunos alias predeterminados:

```
(global) close : exit
(global) quit : exit
(global) bye : exit
warnlog : tools log events
virlog : tools log detections
registro de antivirus a petición : herramientas para explorar registros
```

“(global)” significa que el comando puede usarse en cualquier parte sin importar el contexto actual. Un comando puede tener varios alias asignados, por ejemplo, el comando `EXIT` tiene alias `CLOSE`, `QUIT` y `BYE`. Cuando desea salir de eShell, puede usar el comando `EXIT` o cualquiera de sus alias. El alias `VIRLOG` es un alias para el comando `DETECTIONS`, que se ubica en el contexto `TOOLS LOG`. De esta forma, el comando `DETECTIONS` está disponible desde `ROOT`, por lo que es más fácil acceder a este (no es necesario ingresar `HERRAMIENTAS` y luego el contexto `LOG` para ejecutarlo directamente desde `ROOT`).

eShell le permite definir su propio alias. El comando `ALIAS` puede localizarse en el contexto de la `INTERFAZ DEL USUARIO DE ESHELL`.

Configuraciones protegidas por contraseña

Las configuraciones de ESET Mail Security pueden estar protegidas por una contraseña. Puede establecer la [contraseña con la interfaz gráfica de usuario](#) o eShell por medio del comando `configurar acceso a la interfaz de usuario bloquear contraseña`. Luego, deberá ingresar esta contraseña, de forma interactiva, para algunos comandos (como aquellos que cambian las configuraciones o modifican datos). Si planea trabajar con eShell por un período más prolongado y no desea ingresar la contraseña de forma repetida, puede hacer que eShell recuerde la contraseña por medio del comando `establecer contraseña`. Su contraseña se completará automáticamente para cada comando ejecutado que la requiera. La contraseña se recordará hasta que salga de eShell, esto quiere decir que deberá usar el comando `establecer contraseña` nuevamente cuando inicie una nueva sesión y desee que eShell recuerde su contraseña.

Guía / Ayuda

Cuando ejecuta el comando `GUIDE` o `HELP`, mostrará la pantalla de “primera vista” donde se explica cómo usar eShell. El comando está disponible desde el contexto `ROOT (eShell>)`.

Historial de comandos

eShell mantiene un historial de los comandos ejecutados previamente. Solo se aplica a los comandos de la sesión interactiva de eShell actual. Cuando haya salido de eShell, el historial de comandos quedará vacío. Use las flechas Arriba y Abajo del teclado para desplazarse por el historial. Al encontrar el comando que buscaba, puede ejecutarlo nuevamente o modificarlo sin necesidad de escribir el comando completo desde el comienzo.

CLS / Borrar los datos de la pantalla

El comando `CLS` puede usarse para borrar la pantalla. Funciona de la misma manera que con el Símbolo de comandos de Windows o interfaces de línea de comandos similares.

EXIT / CLOSE / QUIT / BYE

Para cerrar o salir de eShell, puede usar cualquiera de estos comandos (`EXIT`, `CLOSE`, `QUIT` o `BYE`).

3.7.5.2 Comandos

Esta sección enumera algunos comandos eShell básicos con descripciones como ejemplo.

NOTA

los comandos no distinguen mayúsculas de minúsculas; puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Comandos de ejemplo (incluidos en el contexto ROOT):

ABOUT

Presenta una lista informativa acerca del programa. Muestra información como:

- Nombre del producto de seguridad de ESET instalado y el número de la versión.
- Sistema operativo y detalles del hardware básicos.
- Nombre de usuario (dominio incluido), nombre completo del equipo (FQDN, si el servidor es miembro de un dominio(y nombre de Puesto.
- Los componentes instalados del producto de seguridad de ESET, incluyendo el número de la versión de cada componente.

RUTA CONTEXTUAL:

```
root
```

PASSWORD

Normalmente, para ejecutar comandos protegidos por contraseña, el programa le solicita ingresar una contraseña por razones de seguridad. Esto se aplica a los comandos que deshabilitan la protección antivirus y a los que pueden afectar la configuración de ESET Mail Security. Cada vez que ejecute este tipo de comandos, se le solicitará que ingrese una contraseña. Puede definir la contraseña para evitar tener que ingresar la contraseña todas las veces. eShell la recordará y se usará en forma automática cuando se ejecute un comando protegido por contraseña.

NOTA

la contraseña definida funciona únicamente para la sesión interactiva actual de eShell. Al salir de eShell, la contraseña definida perderá su vigencia. Cuando vuelva a iniciar eShell, deberá definir nuevamente la contraseña.

La contraseña definida también se puede usar al ejecutar archivos o scripts por lotes sin firmar. Asegúrese de establecer la [Directiva de ejecución del shell de ESET](#) para tener **Acceso completo** al ejecutar archivos por lote sin firmar. Aquí se muestra un ejemplo de un archivo de procesamiento por lotes de ese tipo:

```
eshell set password plain <yourpassword> "&" set status disabled
```

Este comando concatenado define la contraseña y deshabilita la protección.

IMPORTANTE

Recomendamos que use archivos por lote firmados, si es posible. De esta manera, evitará tener una contraseña sin formato en el archivo por lotes (su utiliza el método descrito anteriormente). Consulte [Archivos por lote/ Secuencia de comandos](#) (sección **Archivos por lote firmados**) para obtener más detalles.

RUTA CONTEXTUAL:

```
root
```

SINTAXIS:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERACIONES:

`get` : mostrar la contraseña

`set` : establecer o borrar la contraseña

`restore` : borrar la contraseña

ARGUMENTOS:

`plain` : cambiar al ingreso de la contraseña como un parámetro

`password` : contraseña

EJEMPLOS:

`set password plain <yourpassword>` : establece la contraseña que se usará para los comandos protegidos por contraseña

`restore password` : borra la contraseña

EJEMPLOS:

`get password` : use este comando para ver si la contraseña está configurada o no (se indica mediante una estrella "*", pero no muestra la contraseña), cuando no hay ninguna estrella visible, significa que la contraseña no está establecida

`set password plain <yourpassword>` : use este comando para establecer la contraseña definida

`restore password` : este comando borra la contraseña definida

ESTADO

Muestra información acerca del estado de protección actual de ESET Mail Security (similar a la interfaz gráfica de usuario).

RUTA CONTEXTUAL:

`root`

SINTAXIS:

`[get] | restore status`

`set status disabled | enabled`

OPERACIONES:

`get` : mostrar el estado de la protección antivirus

`set` : deshabilitar/habilitar la protección antivirus

`restore` : restaura la configuración predeterminada

ARGUMENTOS:

`disabled` : deshabilitar la protección antivirus

`enabled` : habilitar la protección antivirus

EJEMPLOS:

`get status` : muestra el estado de protección actual

`set status disabled` : deshabilita la protección

`restore status` : restaura la protección a la configuración predeterminada (habilitada)

VIRLOG

Es un alias del comando `DETECTIONS`. Es útil cuando se necesita ver información sobre las infiltraciones detectadas.

WARNLOG

Es un alias del comando `EVENTS`. Es útil cuando se necesita ver información sobre diversos sucesos.

3.7.5.3 Archivos por lotes/ Cifrado

Puede usar eShell como una herramienta poderosa de cifrado para automatización. Para usar el archivo por lotes con eShell, cree uno con un eShell y realice comandos en él. Por ejemplo:

```
eshell obtener estado de antivirus
```

También puede vincular comandos, lo cual a veces es necesario. Por ejemplo, si desea obtener el tipo de una tarea programada específica, escriba lo siguiente:

```
eshell seleccionar tarea programada 4 "&" obtener acción de tareas programadas
```

La selección del elemento (tarea número 4 en este caso) por lo general se aplica solo a una instancia de eShell que se esté ejecutando. Si quisiera ejecutar estos dos comandos uno tras otro, el segundo comando fallaría con el error "No hay tarea seleccionada o la tarea seleccionada ya no existe".

Por razones de seguridad, la [directiva de ejecución](#) está configurada en forma predeterminada para **Comando de ejecución limitado**. Esto le permite usar eShell como una herramienta de supervisión, pero no le permitirá realizar cambios en la configuración de ESET Mail Security con la ejecución de comandos. Si intenta ejecutar un comando con comandos que pueden afectar a la seguridad, como desactivar la protección, verá el mensaje **Acceso denegado**. Si desea ejecutar los comandos que realizan cambios en la configuración, se recomienda usar archivos por lotes firmados.

Si, por algún motivo específico, necesita poder cambiar la configuración con un comando único ingresado en forma manual en el Símbolo de comandos de Windows, tiene que otorgarle a eShell acceso completo (no recomendado). Para otorgar el acceso completo, use el comando `eshell` de política de ejecución de shell en el modo interactivo de eShell o puede hacerlo a través de la interfaz gráfica del usuario en **Configuración avanzada > Interfaz de usuario > [ESET Shell](#)**.

Archivos por lotes firmados

eShell le permite asegurar archivos por lotes comunes (*.bat) con una firma. Los scripts se firman con la misma contraseña que se usa para proteger las configuraciones. Para firmar un script primero debe habilitar la [protección de las configuraciones](#). Puede hacerlo a través de la interfaz gráfica del usuario o desde eShell por medio del comando `configurar acceso a la interfaz de usuario bloquear contraseña`. Una vez que la contraseña de protección de las configuraciones esté configurada puede comenzar a firmar los archivos por lotes.

Para firmar un archivo por lotes, ejecute `firmar <script.bat>` desde el contexto raíz de eShell, en el que *script.bat* es la ruta al script que desea firmar. Ingrese y confirme la contraseña que se usará para firmar. Esta contraseña debe coincidir con la contraseña de protección de las configuraciones. La firma se coloca al final del archivo por lotes en forma de un comando. Si este script ya ha sido firmado, la firma será reemplazada por una nueva.

NOTA

al modificar un archivo por lotes que ya ha sido firmado, debe volver a firmarlo.

NOTA

si cambia la contraseña de [protección de las configuraciones](#), debe volver a firmar todos los scripts, de lo contrario estos no se ejecutarán desde el momento en que cambie la contraseña de protección de las configuraciones. Esto se debe a que la contraseña ingresada al firmar el script debe coincidir con la contraseña de protección de las configuraciones en el sistema destino.

Para ejecutar un archivo por lotes firmado desde el Símbolo de comandos de Windows o como una tarea programada, use el siguiente comando:

```
ejecutar eshell <script.bat>
```

Donde *script.bat* es la ruta al archivo por lotes. Por ejemplo `ejecución de eshell d:\myeshellscript.bat`

3.7.6 ESET SysInspector

[ESET SysInspector](#) es una aplicación que inspecciona minuciosamente su equipo, recopila información detallada sobre los componentes del sistema (como las aplicaciones y los controladores instalados, las conexiones de red o las entradas de registro importantes) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa del comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de códigos maliciosos.

La ventana ESET SysInspector muestra la siguiente información sobre los registros creados:

- **Hora:** la hora de creación del registro.
- **Comentario:** un breve comentario.
- **Usuario:** el nombre del usuario que creó el registro.
- **Estado:** el estado de la creación del registro.

Están disponibles las siguientes opciones:

- **Abrir:** abre el registro creado. También puede hacerlo si hace clic con el botón secundario en el registro creado y luego selecciona **Mostrar** en el menú contextual.
- **Comparar:** compara dos registros existentes.
- **Crear:** crea un registro nuevo. Espere hasta que el registro de ESET SysInspector se haya completado (cuando su **Estado** sea Creado).
- **Eliminar:** elimina los registros seleccionados de la lista.

Al hacer un clic con el botón secundario en uno o varios registros seleccionados, se ofrecen las siguientes opciones desde el menú contextual:

- **Mostrar:** abre el registro seleccionado en ESET SysInspector (equivale a hacer doble clic en el registro).
- **Comparar:** compara dos registros existentes.
- **Crear:** crea un registro nuevo. Espere hasta que el registro de ESET SysInspector se haya completado (cuando su **Estado** sea Creado).
- **Eliminar:** elimina los registros seleccionados de la lista.
- **Eliminar todo:** elimina todos los registros.
- **Exportar:** exporta el registro a un archivo *.xml* o *.xml* comprimido.

3.7.6.1 Creación de una instantánea de estado del equipo

Ingrese un breve comentario que describa el registro que se va a crear y haga clic en el botón **Agregar**. Espere hasta que el registro de ESET SysInspector se haya completado (cuando su estado sea Creado). La creación del registro puede llevar bastante tiempo, según la configuración del hardware y los datos del sistema.

3.7.6.2 ESET SysInspector

3.7.6.2.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el equipo a fondo y muestra los datos recopilados en forma exhaustiva. La información sobre los controladores y aplicaciones instalados, las conexiones de red o las entradas de registro importantes, por ejemplo, puede ayudarle en la investigación de un comportamiento sospechoso del sistema, ya sea debido a incompatibilidades del software o hardware o a una infección por malware.

Puede acceder a ESET SysInspector de dos maneras: Desde la versión integrada en las soluciones ESET Security o mediante la descarga de la versión autosostenible (SysInspector.exe) sin cargo desde el sitio Web de ESET. Ambas versiones tienen una función idéntica y cuentan con los mismos controles del programa. La única diferencia radica en el manejo de los resultados. Tanto la versión autosostenible como la integrada permiten exportar instantáneas del sistema a un archivo *.xml* y guardarlas en el disco. Sin embargo, la versión integrada también permite almacenar las instantáneas del sistema directamente en **Herramientas > ESET SysInspector** (excepto ESET Remote Administrator). Para obtener más información, consulte la sección [ESET SysInspector como parte de ESET Mail Security](#).

Aguarde un momento mientras ESET SysInspector explora el equipo. Puede tardar de 10 segundos a unos minutos

según la configuración del hardware, el sistema operativo y la cantidad de aplicaciones instaladas en el equipo.

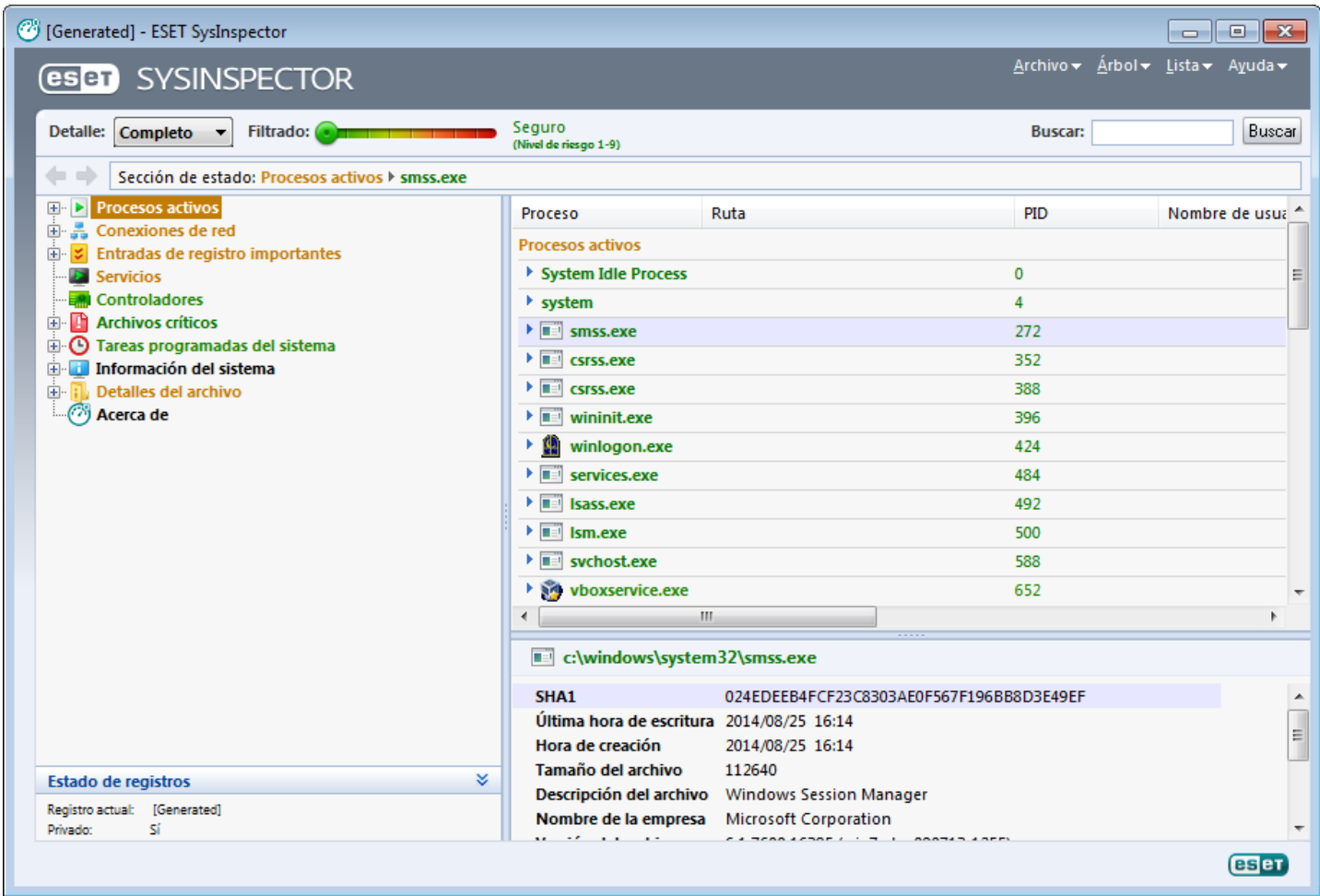
3.7.6.2.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector, simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio Web de ESET. Si ya tiene instalada alguna de las soluciones ESET Security, puede ejecutar ESET SysInspector directamente desde el menú Inicio (haga clic en **Programas > ESET > ESET Mail Security**).

Espere mientras la aplicación examina el sistema. Puede tardar varios minutos.

3.7.6.2.2 Interfaz del usuario y uso de la aplicación

Para lograr una mayor claridad, la ventana principal del programa se divide en cuatro secciones principales: la sección de controles del programa, situada en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana de descripción, situada a la derecha; y la ventana de detalles, situada en la parte inferior de la ventana principal del programa. La sección Estado de registros muestra una lista de los parámetros básicos de un registro (filtro utilizado, tipo de filtro, si el registro es el resultado de una comparación, etc.).



3.7.6.2.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo

Al hacer clic en **Archivo**, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable generar un registro **Adecuado para enviar**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del equipo, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA: Para abrir los informes de ESET SysInspector almacenados previamente, simplemente arrástrelos y suéltelos

en la ventana principal del programa.

Árbol

Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista

Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda

Contiene información sobre la aplicación y sus funciones.

Detalle

Esta configuración afecta la información mostrada en la ventana principal del programa para que resulte más sencillo trabajar con dicha información. En el modo "Básico", el usuario tiene acceso a información utilizada para buscar soluciones a problemas comunes del sistema. En el modo "Medio", el programa muestra detalles menos usados. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se encuentra en el extremo izquierdo (nivel de riesgo 1), se muestran todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos menos peligrosos que el nivel de riesgo actual y muestra solo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante se encuentra en el extremo derecho, el programa muestra únicamente los elementos dañinos conocidos.

Todos los elementos cuyo riesgo designado está entre 6 y 9 pueden suponer un riesgo para la seguridad. Si no está utilizando una solución de seguridad de ESET, es recomendable explorar su sistema con [ESET Online Scanner](#) cuando ESET SysInspector encuentre un elemento de este tipo. ESET Online Scanner es un servicio gratuito.

NOTA: el nivel de riesgo de un elemento se puede determinar rápidamente si se compara el color del elemento con el color del control deslizante del nivel de riesgo.

Comparación

Cuando compara dos registros, puede seleccionar mostrar todos los elementos, mostrar solo elementos agregados, mostrar solo elementos eliminados o mostrar solo elementos reemplazados.

Buscar

Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre o parte del nombre. Los resultados de la solicitud de búsqueda aparecerán en la ventana de descripción.

Volver


Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana de descripción. Puede utilizar la tecla Retroceso y la tecla Barra espaciadora, en lugar de hacer clic en las flechas Atrás y Adelante.

Sección de estado

Muestra el nodo actual en la ventana de navegación.

Importante: los elementos destacados en rojo son elementos desconocidos, por eso el programa los marca como potencialmente peligrosos. Que un elemento aparezca marcado en rojo no significa que deba eliminar el archivo. Antes de eliminarlo, asegúrese de que el archivo es realmente peligroso o innecesario.

3.7.6.2.2 Navegación por ESET SysInspector

ESET SysInspector divide varios tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional al expandir los subnodos de cada nodo. Para abrir o contraer un nodo, solo tiene que hacer doble clic en el nombre del nodo o en , que se encuentran junto al nombre del nodo. Cuando examine la estructura con forma de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo en la ventana de descripción. Si examina los elementos en la ventana Descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana Detalles.

A continuación, se encuentran las descripciones de los nodos principales de la ventana Navegación e información relacionada en las ventanas Descripción y Detalles.

Procesos activos

Este nodo contiene información sobre aplicaciones y procesos que se ejecutan al generar el registro. En la ventana Descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación y el nivel de riesgo del archivo.

La ventana Detalles contiene información adicional de los elementos seleccionados en la ventana Descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA: Un sistema operativo incluye varios componentes importantes del núcleo que se ejecutan de forma ininterrumpida y que proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos optimizan el inicio previo de dichos procesos; son seguros para el sistema.

Conexiones de red

La ventana Descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red mediante el protocolo seleccionado en la ventana Navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. También puede comprobar las direcciones IP de los servidores DNS.

La ventana Detalles contiene información adicional de los elementos seleccionados en la ventana Descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes

Contiene una lista de entradas de registro seleccionadas que suelen estar asociadas a varios problemas del sistema, como las que especifican programas de arranque, objetos del ayudante de exploración (BHO), etc.

En la ventana Descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana Detalles.

Servicios

La ventana Descripción contiene una lista de archivos registrados como Servicios de Windows. En la ventana Detalles, puede consultar la forma de inicio establecida para el servicio e información específica del archivo.

Controladores

Una lista de los controladores instalados en el sistema.

Archivos críticos

En la ventana Descripción, se muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Tareas programadas del sistema

Contiene una lista de tareas accionadas por las Tareas programadas de Windows en un tiempo/intervalo especificado.

Información del sistema

Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno, los derechos de usuario y registros de sucesos del sistema establecidos.

Detalles del archivo

Una lista de los archivos del sistema y los archivos de la carpeta Archivos de programa importantes. Se puede encontrar información adicional específica de los archivos en las ventanas Descripción y Detalles.

Acerca de

Información sobre la versión de ESET SysInspector y la lista de módulos del programa.

Los accesos directos que se pueden utilizar al trabajar con ESET SysInspector incluyen:

Archivo

Ctrl+O	Abrir el registro existente
Ctrl+S	Guardar los registros creados

Generar

Ctrl+G	Genera una instantánea de estado del equipo estándar
Ctrl+H	Genera una instantánea de estado del equipo que también puede registrar información confidencial

Filtrado de elementos

1, O	Seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9
2	Seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9
3	Seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9
4, U	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9
5	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
-	Disminuir el nivel de riesgo
+	Aumentar el nivel de riesgo
Ctrl+9	Modo de filtrado, mismo nivel o superior
Ctrl+0	Modo de filtrado, solo mismo nivel

Ver

Ctrl+5	Ver por proveedor, todos los proveedores
Ctrl+6	Ver por proveedor, solo Microsoft
Ctrl+7	Ver por proveedor, resto de proveedores
Ctrl+3	Mostrar todos los detalles
Ctrl+2	Mostrar la mitad de los detalles
Ctrl+1	Visualización básica
Retroceso	Volver un paso atrás
Espacio	Continuar con el paso siguiente
Ctrl+W	Expandir el árbol
Ctrl+Q	Contraer el árbol

Otros controles

Ctrl+T	Ir a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl+P	Mostrar la información básica de un elemento
Ctrl+A	Mostrar la información completa de un elemento
Ctrl+C	Copiar el árbol del elemento actual
Ctrl+X	Copiar elementos

Ctrl+B	Buscar información en Internet acerca de los archivos seleccionados
Ctrl+L	Abrir la carpeta en la que se encuentra el archivo seleccionado
Ctrl+R	Abrir la entrada correspondiente en el editor de registros
Ctrl+Z	Copiar una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl+F	Activar el campo de búsqueda
Ctrl+D	Cerrar los resultados de búsqueda
Ctrl+E	Ejecutar el script de servicio

Comparación

Ctrl+Alt+O	Abrir el registro original/comparativo
Ctrl+Alt+R	Cancelar la comparación
Ctrl+Alt+1	Mostrar todos los elementos
Ctrl+Alt+2	Mostrar solo los elementos agregados, el registro incluirá los elementos presentes en el registro actual
Ctrl+Alt+3	Mostrar solo los elementos eliminados, el registro incluirá los elementos presentes en el registro anterior
Ctrl+Alt+4	Mostrar solo los elementos sustituidos (archivos incluidos)
Ctrl+Alt+5	Mostrar solo las diferencias entre los registros
Ctrl+Alt+C	Mostrar la comparación
Ctrl+Alt+N	Mostrar el registro actual
Ctrl+Alt+P	Abrir el registro anterior

Varios

F1	Ver la Ayuda
Alt+F4	Cerrar el programa
Alt+Mayús+F4	Cerrar el programa sin preguntar
Ctrl+I	Estadísticas del registro

3.7.6.2.2.3 Comparación

La característica Comparar le permite al usuario comparar dos registros existentes. El resultado es un conjunto de elementos no comunes a ambos registros. Esta opción es adecuada para realizar un seguimiento de los cambios realizados en el sistema; constituye una herramienta útil para detectar códigos maliciosos.

Una vez iniciada, la aplicación crea un nuevo registro, que aparecerá en una ventana nueva. Haga clic en **Archivo > Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, haga clic en **Archivo > Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro a la vez.

La ventaja de comparar dos registros es que permite ver un registro actualmente activo y un registro guardado en un archivo. Para comparar registros, haga clic en **Archivo > Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en la ventana principal del programa. El registro resultante solo mostrará las diferencias entre esos dos registros.

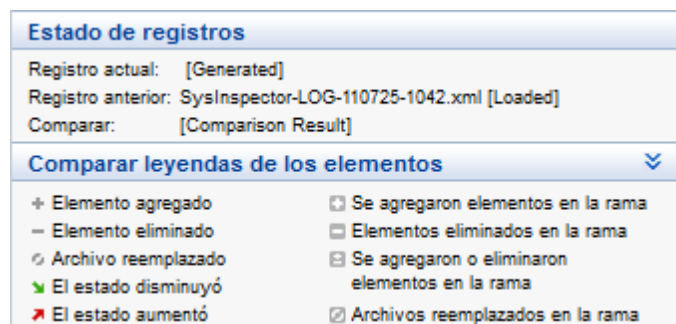
NOTA: Si compara dos archivos de registro, haga clic en **Archivo > Guardar registro** y guárdelo como un archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, se compararán automáticamente los registros que contiene.

Junto a los elementos mostrados, ESET SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

- + nuevo valor que no se encuentra en el registro anterior
- □ la sección de estructura con forma de árbol contiene nuevos valores
- - valor eliminado que solo se encuentra en el registro anterior
- □ la sección de estructura con forma de árbol contiene valores eliminados
- ↻ se cambió un valor o archivo
- □ la sección de estructura con forma de árbol contiene valores o archivos modificados
- ▼ disminuyó el nivel de riesgo o era superior en el registro anterior
- ▲ aumentó el nivel de riesgo o era inferior en el registro anterior

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos y muestra los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirlo posteriormente.

Ejemplo

Genere y guarde un registro, en el que se recopile información original sobre el sistema, en un archivo con el nombre anterior.xml. Después de que se hagan los cambios en el sistema, abra ESET SysInspector y permítale generar un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.

Para realizar un seguimiento de los cambios entre estos dos registros, haga clic en **Archivo > Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado si utiliza la siguiente opción de la línea de comandos:

SysInspector.exe actual.xml anterior.xml

3.7.6.2.3 Parámetros de la línea de comandos

ESET SysInspector es compatible con la generación de informes desde la línea de comandos mediante el uso de estos parámetros:

/gen	generar registro directamente desde la línea de comandos sin iniciar la interfaz gráfica de usuario
/privacy	generar registro omitiendo la información confidencial
/zip	guardar registro resultante en un archivo comprimido zip
/silent	quitar la ventana de progreso al generar el registro desde la línea de comandos
/blank	iniciar SysInspector sin generar o cargar el registro

Ejemplos

Uso:

SysInspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe .\clientlog.xml*

Para generar un registro desde la línea de comandos, utilice: *SysInspector.exe /gen=. \mynewlog.xml*

Para generar un registro en el que se excluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen=. \mynewlog.zip /privacy /zip*

Para comparar dos archivos de registro y examinar las diferencias, utilice: *SysInspector.exe new.xml old.xml*

NOTA: si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

3.7.6.2.4 Script de servicio

El script de servicio es una herramienta que ofrece asistencia a los clientes que utilizan ESET SysInspector mediante la eliminación de objetos no deseados del sistema.

El script de servicio le permite al usuario exportar el registro completo de ESET SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden provocar daños en el sistema operativo.

Ejemplo

Si tiene la sospecha de que el equipo está infectado por un virus que el antivirus no detecta, siga estas instrucciones detalladas:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura con forma de árbol), presione Shift y seleccione el último elemento para marcarlos todos.
3. Haga un clic derecho en los objetos seleccionados y elija **Exportar las secciones seleccionadas a un script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de no marcar ningún archivo u objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo > Ejecutar el script de servicio** e ingrese la ruta en su script.
7. Haga clic en **Aceptar** para ejecutar el script.

3.7.6.2.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga un clic derecho en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione la opción **Exportar todas las secciones al script de servicio** o la opción **Exportar las secciones seleccionadas al script de servicio**.

NOTA: Cuando se comparan dos registros, el script de servicio no se puede exportar.

3.7.6.2.4.2 Estructura del script de servicio

En la primera línea del encabezado del script, encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter "-" situado delante de un elemento por el carácter "+". En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos activos)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se seleccionó (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el

script.

02) Loaded modules (Módulos cargados)

En esta sección se listan los módulos del sistema que se utilizan actualmente.

Ejemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbexb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbexb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrm.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket, lo que libera recursos del sistema.

04) UDP endpoints (Terminales UDP)

En esta sección se incluye información sobre las terminales UDP.

Ejemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Cuando se ejecute, el script aislará al propietario del socket en las terminales UDP marcadas y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
  HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Cuando se ejecute el script, las entradas marcadas se eliminarán, reducirán a valores de 0 bytes o restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se listan los servicios registrados en el sistema.

Ejemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se listan los controladores instalados.

Ejemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Cuando se ejecuta el script, se detienen los controladores seleccionados. Observe que algunos controladores no se permitirán detenerse.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos que son críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

3.7.6.2.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción **Ejecutar el script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el siguiente mensaje: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

Se mostrará una ventana de diálogo para confirmar que el script se ejecutó correctamente.

Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el siguiente mensaje: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione **Sí** para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparecerá una ventana de diálogo con el siguiente mensaje: **El script de servicio seleccionado no está firmado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del equipo. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nueva.

3.7.6.2.5 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

Aunque ESET SysInspector no requiere privilegios de administrador para su ejecución, sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario normal o restringido, se recopilará menor cantidad de información acerca de su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su equipo. Para guardar uno, haga clic en **Archivo > Guardar registro** desde la ventana principal del programa. Los registros se guardan con formato XML. De forma predeterminada, los archivos se guardan en el directorio *%USERPROFILE%\My Documents* con una convención de nomenclatura del tipo de "SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y haga clic en **Archivo > Abrir registro** en la ventana principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, es recomendable crear un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista o 7

no permita la acción de arrastrar y soltar entre ventanas que cuentan con permisos de seguridad diferentes.

¿Existe alguna especificación disponible para el formato del archivo de registro? ¿Y algún conjunto de herramientas para el desarrollo de aplicaciones (SDK)?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas de programación, ya que la aplicación se encuentra aún en fase de desarrollo. Una vez que se haya lanzado, podremos proporcionar estos elementos en función de la demanda y los comentarios por parte de los clientes.

¿Cómo evalúa ESET SysInspector el riesgo que plantea un objeto en particular?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, utiliza una serie de reglas heurísticas que examinan las características de cada uno de los objetos y luego estiman el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor **1: seguro (en color verde)** hasta **9: peligroso" (en color rojo)**. En el panel de navegación que se encuentra a la izquierda, las secciones estarán coloreadas según el nivel máximo de riesgo que presente un objeto en su interior.

El nivel de riesgo "6: desconocido (en color rojo)", ¿significa que un objeto es peligroso?

Las evaluaciones de ESET SysInspector no garantizan que un objeto sea malicioso. Esta determinación deberá confirmarla un experto en seguridad informática. ESET SysInspector está diseñado para proporcionarles a dichos expertos una evaluación rápida, con la finalidad de que conozcan los objetos que deberían examinar en un sistema en busca de algún comportamiento inusual.

¿Por qué ESET SysInspector se conecta a Internet cuando se ejecuta?

Como muchas otras aplicaciones, ESET SysInspector contiene una firma digital que actúa a modo de "certificado". Esta firma sirve para garantizar que ESET desarrolló la aplicación y que no se alteró. Para verificar la autenticidad del certificado, el sistema operativo debe contactar con la autoridad certificadora, que verificará la identidad del desarrollador de la aplicación. Este es un comportamiento normal para todos los programas firmados digitalmente que se ejecutan en Microsoft Windows.

¿En qué consiste la tecnología Anti Stealth?

La tecnología Anti Stealth proporciona un método efectivo de detección de rootkits.

Si códigos maliciosos que se comportan como un rootkit atacan el sistema, el usuario se puede exponer a la pérdida o robo de información. Si no se dispone de una herramienta anti-rootkit especial, es prácticamente imposible detectar los rootkits.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, ESET SysInspector revisa en primer lugar si el archivo contiene una firma digital integrada. Si se encuentra una firma digital, el archivo se validará con esa información. Si no se encuentra una firma digital, ESI comienza a buscar el archivo CAT correspondiente (Catálogo de seguridad: %systemroot%\system32\catroot), que contiene información sobre el archivo ejecutable procesado. Si se encuentra el archivo CAT relevante, la firma digital de dicho archivo CAT será la que se aplique en el proceso de validación del archivo ejecutable.

Esa es la razón por la cual a veces hay archivos marcados como "Firmado por MS", pero que tienen una entrada "Nombre de compañía" diferente.

3.7.6.2.6 ESET SysInspector como parte de ESET Mail Security

Para abrir la sección ESET SysInspector en ESET Mail Security, haga clic en **Herramientas > ESET SysInspector**. El sistema de administración de la ventana de ESET SysInspector es parecido al de los registros de exploración del equipo o las tareas programadas. Se puede obtener acceso a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, eliminar y exportar) con tan solo un par de clics.

La ventana ESET SysInspector contiene información básica acerca de las instantáneas creadas como, por ejemplo, la hora de creación, un breve comentario, el nombre del usuario que creó la instantánea y el estado de la misma.

Para comparar, crear o eliminar instantáneas, utilice los botones correspondientes ubicados debajo de la lista de instantáneas de la ventana ESET SysInspector. Estas opciones también están disponibles en el menú contextual. Para ver la instantánea del sistema seleccionada, utilice la opción del menú contextual **Mostrar**. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón secundario en ella y seleccione **Exportar...**

Abajo se muestra una descripción detallada de las opciones disponibles:

- **Comparar:** le permite comparar dos registros existentes. Esta opción es ideal para realizar un seguimiento de los cambios entre el registro actual y el anterior. Para poder aplicar esta opción, debe seleccionar dos instantáneas con el fin de compararlas.
- **Crear...:** crea un nuevo registro. Antes debe ingresar un breve comentario acerca del registro. Para obtener información sobre el progreso de la creación de la instantánea (que se está generando en ese momento), consulte la columna **Estado**. Todas las instantáneas completadas aparecen marcadas con el estado **Creado**.
- **Eliminar/Eliminar todos:** elimina entradas de la lista.
- **Exportar...:** guarda la entrada seleccionada en un archivo XML (y también en una versión comprimida).

3.7.7 ESET SysRescue Live

ESET SysRescue Live es una utilidad que le permite crear un disco de arranque que contiene una de las soluciones ESET Security, ESET NOD32 Antivirus, ESET Smart Security o algunos de los productos orientados al servidor. La ventaja principal de ESET SysRescue Live es que la solución ESET Security se ejecuta en forma independiente del sistema operativo del host, pero cuenta con acceso directo al disco y al sistema de archivos. De esta forma, es posible quitar las infiltraciones que normalmente no se podrían eliminar, por ejemplo, mientras el sistema operativo está activo, etc.

3.7.8 Programador

Podrá encontrar el **Tareas programadas** en la sección **Herramientas** de la ventana del programa principal. En las tareas programadas se administran y se ejecutan tareas programadas, según los parámetros definidos.

Tareas programadas enumera todas las tareas programadas en forma de tabla y muestra sus parámetros, como tipo de **Tarea**, **Nombre de la tarea**, **Hora de ejecución** y **Última ejecución**. Para obtener más información, haga doble clic sobre una tarea para ver el [Resumen general de tareas programadas](#). Después de la instalación, hay un conjunto de tareas predefinidas. También puede crear nuevas tareas programadas si hace clic en [Agregar tarea](#).

Cuando hace clic con el botón secundario sobre una tarea, puede elegir la acción que desea realizar. Las acciones disponibles son:

Mostrar detalles de la tarea

Ejecutar ahora

Agregar...

Editar...

Eliminar

Use la casilla de verificación junto a la tarea para activarla/desactivarla. Para editar la configuración de una tarea programada, haga un clic con el botón secundario en la tarea y luego en **Editar...** o seleccione la tarea que quiera modificar y haga clic en **Editar**.

MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

✓

CONTROL

📄

ARCHIVOS DE REGISTRO

🔍

EXPLORAR

✉️

CUARENTENA DE CORREO

🔄

ACTUALIZACIÓN

⚙️

CONFIGURACIÓN

🛠️

HERRAMIENTAS

?

AYUDA Y SOPORTE

←

Tareas programadas

☰

☐

?

Tarea	Nombre	Hora de inicio	Última ejecución
<input checked="" type="checkbox"/>	Mantenimiento de reg...	Mantenimiento de registros La tarea se ejecutará todo...	25-Aug-15 3:35:05 PM
<input checked="" type="checkbox"/>	Actualización	Actualización automática ... La tarea se ejecutará reiter...	25-Aug-15 4:35:06 PM
<input checked="" type="checkbox"/>	Actualización	Actualización automática ... Conexión por módem a In...	
<input type="checkbox"/>	Actualización	Actualización automática ... El usuario inicie la sesión (...)	
<input checked="" type="checkbox"/>	Verificación de archiv...	Verificación de archivos d... El usuario inicie la sesión ...	25-Aug-15 3:37:36 PM
<input checked="" type="checkbox"/>	Verificación de archiv...	Verificación de archivos d... Se haya actualizado corre...	25-Aug-15 4:35:29 PM
<input checked="" type="checkbox"/>	Primera exploración	Primera exploración auto... La tarea se ejecutará una s...	25-Aug-15 3:54:06 PM

Agregar tarea

Editar

Eliminar

ENJOY SAFER TECHNOLOGY™

Las tareas programadas predeterminadas (predefinidas) son:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática después de la conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**
- **Exploración automática de archivos durante el inicio del sistema** (después del registro del usuario)
- **Exploración automática de archivos durante el inicio del sistema** (tras la actualización correcta de la base de datos de firmas de virus)
- **Primera exploración automática**

3.7.8.1 Programador: agregar tarea

Para crear una nueva tarea en el Programador, haga clic en el botón **Agregar tarea** o clic con el botón secundario y seleccione **Agregar** en el menú contextual. Se abrirá un asistente que lo ayudará a crear una tarea programada. A continuación, se describe un procedimiento paso a paso:

1. Ingrese el **Nombre de la tarea** y seleccione el **Tipo de tarea** que desee del menú desplegable:

- **Ejecutar aplicación externa:** programa la ejecución de una aplicación externa.
- **Mantenimiento de registros:** los archivos de registro también contienen remanentes de registros eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema:** verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo:** crea una instantánea del equipo de [<%ESI%>](#), que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a petición:** realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Primera exploración:** de manera predeterminada, 20 minutos después de la instalación o reinicio se realizará una exploración del equipo como una tarea de prioridad baja.
- **Actualizar:** programa una tarea de actualización mediante la actualización de la base de datos de firmas de virus y los módulos del programa.
- **Exploración de la base de datos:** le permite programar una exploración de la base de datos y elegir elementos para ser explorados. Básicamente, es una [Exploración de la base de datos a petición](#).

NOTA

Si usted tiene la [protección de base de datos de la casilla de correo](#) habilitada, todavía puede programar esta tarea, pero finalizará con un mensaje de error que se mostrará en la sección [Exploración](#) de la GUI principal que dice **Exploración de la base de datos - Exploración interrumpida debido a un error**. Para evitar esto, debe asegurarse de que la protección de la base de datos de la casilla de correo esté deshabilitada durante el horario en que la **Exploración de la base de datos** se programó para su ejecución.

- **Enviar informes de cuarentena de correo:** programa un [Informe de cuarentena de correo para enviarse por correo electrónico](#).
 - **Exploración en segundo plano:** le da la oportunidad al servidor Exchange Server de [ejecutar una exploración de la base de datos en segundo plano](#) de ser necesario.
2. Si desea desactivar la tarea después de crearla, haga clic en el interruptor junto a **Habilitado**. Podrá activar la tarea más tarde mediante la casilla de verificación en la vista [Tareas programadas](#). Haga clic en **Siguiente**.
3. Seleccione cuándo desea que la **Tarea programada se ejecute**:
- **Una vez:** la tarea se realizará solo una vez en una fecha y hora específica.
 - **Reiteradamente:** la tarea se realizará con el intervalo de tiempo especificado (en minutos).
 - **Diariamente:** la tarea se ejecutará reiteradamente todos los días a la hora especificada.
 - **Semanalmente:** la tarea se ejecutará una o varias veces a la semana, en los días y a la hora especificados.
 - **Cuando se cumpla la condición:** la tarea se ejecutará luego de un suceso especificado.
4. Si quiere evitar que la tarea se ejecute cuando el sistema funciona a batería (por ejemplo, UPS), haga clic en el interruptor junto a **Omitir tarea al ejecutar con alimentación de la batería**. Haga clic en **Siguiente**.
5. Si la tarea no se pudo ejecutar en el tiempo programado, puede elegir cuándo se ejecutará:
- **A la siguiente hora programada**
 - **Lo antes posible**
 - **Inmediatamente, si el tiempo desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el uso del selector **Tiempo desde la última ejecución**)
6. Haga clic en **Siguiente**. Según el tipo de tarea, podría ser necesario especificar los **Detalles de la tarea**. Una vez finalizado, haga clic en el botón **Terminar**. La nueva tarea programada aparecerá en la vista de [Tareas programadas](#).

3.7.9 Enviar muestras para su análisis

El cuadro de diálogo para el envío de muestras le permite enviar un archivo o un sitio a ESET para su análisis y puede encontrarse en **Herramientas > Enviar el archivo para su análisis**. Si encuentra un archivo de conducta sospechosa en su equipo o un sitio sospechoso en Internet, puede enviarlo al laboratorio de virus de ESET para su análisis. Si el archivo resulta ser una aplicación o un sitio maliciosos, se agregará su detección a una de las próximas actualizaciones.

Como alternativa, puede enviar el archivo por correo electrónico. Para hacerlo, comprima los archivos con WinRAR o WinZIP, protéjalos con la contraseña “infected” y envíelos a samples@eset.com. Recuerde usar un tema descriptivo e incluir la mayor cantidad de información posible sobre el archivo (por ejemplo, el sitio web desde donde realizó la descarga).

NOTA

antes de enviar una muestra a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:

- el programa directamente no detecta el archivo o el sitio web
- el programa detecta erróneamente el archivo o el sitio web como una amenaza

No recibirá una respuesta a menos que se requiera más información para el análisis.

Seleccione la descripción del menú desplegable **Motivo por el cual se envía la muestra** que mejor se adapte a su mensaje:

- [Archivo sospechoso](#)
- [Sitio sospechoso](#) (un sitio web que se encuentra infectado por un malware)
- [Archivo falso positivo](#) (un archivo que se detecta como una infección pero que no está infectado)
- [Sitio falso positivo](#)
- [Otros](#)

Archivo/sitio: la ruta al archivo o sitio web que desea enviar.

Correo electrónico de contacto: el correo electrónico de contacto se envía junto con los archivos sospechosos a ESET y puede usarse para contactarlo en caso de que se requiera información adicional para el análisis. El ingreso del correo electrónico de contacto es opcional. No obtendrá una respuesta de ESET a menos que se requiera más información, ya que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos.

3.7.9.1 Archivo sospechoso

Signos y síntomas observados de infección de malware: ingrese una descripción sobre la conducta de los archivos sospechosos observada en el equipo.

Origen del archivo (dirección URL o proveedor): ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Notas e información adicional: aquí puede ingresar información adicional o una descripción útil para el proceso de identificación del archivo sospechoso.

NOTA

aunque solo el primer parámetro es obligatorio (**Signos y síntomas observados de infección de malware**), el suministro de información adicional ayudará en forma significativa a nuestros laboratorios en el proceso de identificación de las muestras.

3.7.9.2 Sitio sospechoso

Seleccione una de las siguientes opciones del menú desplegable **Problemas del sitio**:

- **Infectado**: un sitio web que contiene virus u otro malware distribuidos por varios métodos.
- **Phishing**: suele usarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc. Lea más información sobre este tipo de ataque en el [glosario](#).
- **Fraudulento**: un sitio web fraudulento o engañoso.
- Seleccione **Otro** si las opciones mencionadas previamente no se aplican al sitio que va a enviar.

Notas e información adicional: aquí puede ingresar información adicional o una descripción útil para el análisis del sitio web sospechoso.

3.7.9.3 Archivo falso positivo

Le solicitamos que envíe los archivos detectados como una infección pero no se encuentran infectados para mejorar nuestro motor antivirus y antispyware y ayudar con la protección de los demás. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en la base de datos de firmas de virus.

Nombre y versión de la aplicación: el título del programa y su versión (por ejemplo, número, alias o nombre del código).

Origen del archivo (dirección URL o proveedor): ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Propósito de la aplicación: la descripción general de la aplicación, el tipo de aplicación (por ej., navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional: aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

NOTA

los primeros tres parámetros se requieren para identificar aplicaciones legítimas y distinguirlas del código malicioso. Al proporcionar información adicional, ayudará significativamente a nuestros laboratorios en el proceso de identificación y en el procesamiento de las muestras.

3.7.9.4 Sitio falso positivo

Le recomendamos que envíe los sitios que se detectan como infectados, fraudulentos o phishing pero que no lo son. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en la base de datos de firmas de virus. Envíenos esta página web para mejorar nuestro motor antivirus y antiphishing y ayudar a proteger a los demás.

Notas e información adicional: aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

3.7.9.5 Otros

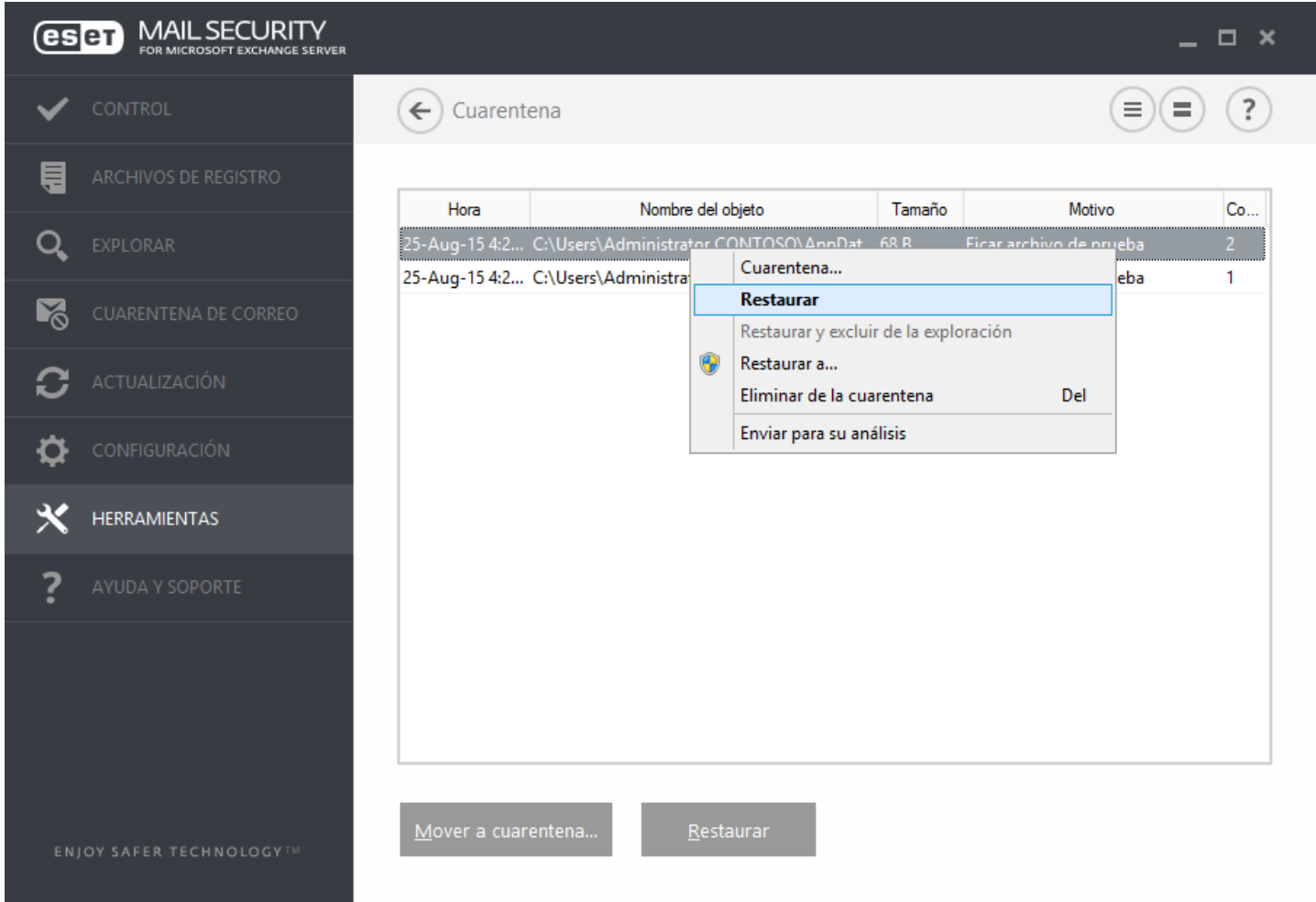
Use este formulario si el archivo no se puede categorizar como **Archivo sospechoso** o **Falso positivo**.

Motivo por el cual se envía el archivo: ingrese una descripción detallada y el motivo por el cual envía el archivo.

3.7.10 Cuarentena

La función principal de la cuarentena consiste en almacenar los archivos infectados en forma segura. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o en caso de que ESET Mail Security los esté detectado erróneamente.

Puede elegir poner cualquier archivo en cuarentena. Esta acción es recomendable cuando un archivo se comporta de manera sospechosa pero la exploración antivirus no lo detecta. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena pueden visualizarse en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta a la ubicación original de los archivos infectados, su tamaño en bytes, el motivo (por ejemplo, objeto agregado por el usuario) y la cantidad de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias infiltraciones).

En caso de que los objetos del mensaje de correo electrónico estén en cuarentena en la cuarentena de archivos, se muestra la información en forma de ruta a la casilla de correo/carpeta/nombre de archivo.

3.8 Ayuda y soporte

ESET Mail Security contiene herramientas de solución de problemas e información de soporte que lo ayudarán a resolver los problemas que puedan surgir.

Ayuda

- **Buscar en la base de conocimientos de ESET:** la [base de conocimiento de ESET](#) contiene respuestas a las preguntas más frecuentes y soluciones recomendadas para varios problemas. La actualización regular por parte de los especialistas técnicos de ESET convierte a la base de conocimiento en la herramienta más potente para resolver varios tipos de problemas.
- **Abrir la ayuda:** haga clic en este vínculo para abrir las páginas de ayuda de ESET Mail Security.
- **Respuestas rápidas a consultas frecuentes:** seleccione esta opción para buscar soluciones a los problemas más frecuentes. Es recomendable leer esta sección antes de ponerse en contacto con el equipo de soporte técnico.

Atención al cliente

- **Enviar una solicitud de soporte:** si no pudo encontrar una respuesta a su problema, también puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con nuestro departamento de Atención al cliente.

Herramientas de soporte

- **Enciclopedia de amenazas :** vínculos a la Enciclopedia de amenazas de ESET, que contiene información sobre los peligros y síntomas de los diferentes tipos de infiltración.
- **Recolector de registros de ESET:** enlaces a la [página de descarga](#) del Recolector de registros de ESET. Log Collector es una aplicación que recolecta la información en forma automática, tal como la configuración y los registros de su servidor para ayudar a resolver los problemas más rápidamente. Para obtener más información acerca del Recolector de registros de ESET, visite la [Ayuda en línea](#).
- **Historial de la base de datos de firmas de virus:** vínculos al Radar de virus de ESET, que contiene información acerca de las versiones de la base de datos de firmas de virus de ESET.
- **Limpiador especializado de ESET:** este limpiador identifica y elimina automáticamente las infecciones de malware comunes; para obtener más información visite este artículo de la [Base de conocimiento de ESET](#).

Información acerca del producto y la licencia

- **Acerca de ESET Mail Security:** muestra la información acerca de una copia de [ESET Mail Security](#).
- **Administrar licencia:** haga clic para abrir la ventana de activación del producto. Seleccione uno de los métodos disponibles para activar ESET Mail Security. Consulte [Cómo activar ESET Mail Security](#) para obtener más información.

3.8.1 Cómo

Este capítulo abarca las preguntas más frecuentes y los problemas que se pueden encontrar. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

[Cómo actualizar ESET Mail Security](#)

[Cómo activar ESET Mail Security](#)

[Cómo programar una tarea de exploración \(cada 24 horas\)](#)

[Cómo quitar un virus del servidor](#)

[Cómo funciona una exclusión automática](#)

Si el problema no está contemplado en las páginas de ayuda indicadas anteriormente, intente buscarlo por palabra

clave o mediante una frase descriptiva en las páginas de ayuda de ESET Mail Security.

Si no encuentra la solución al problema o la pregunta en las páginas de ayuda, intente buscarlo en nuestra [Base de conocimiento](#) en línea, que se actualiza con regularidad.

En caso de ser necesario, también puede ponerse en contacto directamente con nuestro centro de soporte técnico en línea para consultar sus preguntas o problemas. Puede encontrar el formulario de contacto en la ficha Ayuda y soporte de su programa de ESET.

3.8.1.1 Cómo actualizar ESET Mail Security


La actualización de ESET Mail Security se puede realizar en forma manual o automática. Para iniciar la actualización, haga clic en **Actualizar la base de datos de firmas de virus**. La encontrará en la sección **Actualización** del programa.

La configuración predeterminada de la instalación crea una tarea de actualización automática que se ejecuta cada hora. Si necesita cambiar el intervalo, vaya a **Tareas programadas** (para obtener más información sobre las tareas programadas, [haga clic aquí](#)).

3.8.1.2 Cómo activar ESET Mail Security


Luego de que la instalación se complete, se le solicitará que active el producto.

Hay varios métodos para activar su producto. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar según el país, así como de los medios de distribución (CD/DVD, página web de ESET, etc.).

Para activar su copia de ESET Mail Security directamente desde el programa, haga clic en el ícono de la bandeja del sistema  y seleccione **El producto no está activado** del menú. También puede activar su producto desde el menú principal en **Ayuda y soporte > Activar el producto** o estado de **Seguimiento > El producto no está activado**.

Puede usar cualquiera de los siguientes métodos para activar ESET Mail Security:

- **Clave de licencia:** una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se usa para identificar al propietario de la licencia y para activarla.
- **Security Admin:** una cuenta creada en el [portal ESET License Administrator](#) con credenciales (dirección de correo electrónico + contraseña). Este método le permite administrar múltiples licencias desde una ubicación.
- Archivo de **Licencia sin conexión:** un archivo generado automáticamente que será transferido al producto de ESET para brindar información sobre la licencia. Su licencia sin conexión se genera desde el portal de licencias y se usa en los entornos donde la aplicación no puede conectarse con la autoridad otorgante.
- Haga clic en **Activar más tarde** con Remote Administrator de ESET si su equipo es miembro de una red administrada y su administrador realizará la activación remota a través de ESET Remote Administrator. Además, puede utilizar esta opción si desea activar este cliente más tarde.

Seleccione **Ayuda y soporte > Administrar licencia** en la ventana principal del programa para administrar la información de su licencia en cualquier momento. Verá la ID pública de la licencia usada por ESET para identificar su producto y para la identificación de la licencia. El nombre de usuario bajo el cual su equipo está registrado se almacena en la sección **Acerca de** que puede visualizar al hacer clic con el botón derecho en el ícono de la bandeja del sistema .

NOTA

ESET Remote Administrator tiene la capacidad de activar equipos de clientes de manera silenciosa con el uso de licencias que el administrador pone a disposición.

3.8.1.3 Cómo ESET Mail Security cuenta los buzones de correo

Para obtener detalles consulte nuestro [Artículo de la base de conocimiento](#).

3.8.1.4 Cómo crear una nueva tarea en Tareas programadas

Para crear una nueva tarea en el Programador, haga clic en el botón **Agregar tarea** o clic con el botón secundario y seleccione **Agregar** en el menú contextual. Se abrirá un asistente que lo ayudará a crear una tarea programada. A continuación, se describe un procedimiento paso a paso:

1. Ingrese el **Nombre de la tarea** y seleccione el **Tipo de tarea** que desee del menú desplegable:

- **Ejecutar aplicación externa:** programa la ejecución de una aplicación externa.
- **Mantenimiento de registros:** los archivos de registro también contienen remanentes de registros eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema:** verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo:** crea una instantánea del equipo de [<%ESI%>](#), que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a petición:** realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Primera exploración:** de manera predeterminada, 20 minutos después de la instalación o reinicio se realizará una exploración del equipo como una tarea de prioridad baja.
- **Actualizar:** programa una tarea de actualización mediante la actualización de la base de datos de firmas de virus y los módulos del programa.
- **Exploración de la base de datos:** le permite programar una exploración de la base de datos y elegir elementos para ser explorados. Básicamente, es una [Exploración de la base de datos a petición](#).

NOTA

Si usted tiene la [protección de base de datos de la casilla de correo](#) habilitada, todavía puede programar esta tarea, pero finalizará con un mensaje de error que se mostrará en la sección [Exploración](#) de la GUI principal que dice **Exploración de la base de datos - Exploración interrumpida debido a un error**. Para evitar esto, debe asegurarse de que la protección de la base de datos de la casilla de correo esté deshabilitada durante el horario en que la **Exploración de la base de datos** se programó para su ejecución.

- **Enviar informes de cuarentena de correo:** programa un [Informe de cuarentena de correo para enviarse por correo electrónico](#).
 - **Exploración en segundo plano:** le da la oportunidad al servidor Exchange Server de [ejecutar una exploración de la base de datos en segundo plano](#) de ser necesario.
2. Si desea desactivar la tarea después de crearla, haga clic en el interruptor junto a **Habilitado**. Podrá activar la tarea más tarde mediante la casilla de verificación en la vista [Tareas programadas](#). Haga clic en **Siguiente**.
3. Seleccione cuándo desea que la **Tarea programada se ejecute**:
- **Una vez:** la tarea se realizará solo una vez en una fecha y hora específica.
 - **Reiteradamente:** la tarea se realizará con el intervalo de tiempo especificado (en minutos).
 - **Diariamente:** la tarea se ejecutará reiteradamente todos los días a la hora especificada.
 - **Semanalmente:** la tarea se ejecutará una o varias veces a la semana, en los días y a la hora especificados.
 - **Cuando se cumpla la condición:** la tarea se ejecutará luego de un suceso especificado.
4. Si quiere evitar que la tarea se ejecute cuando el sistema funciona a batería (por ejemplo, UPS), haga clic en el interruptor junto a **Omitir tarea al ejecutar con alimentación de la batería**. Haga clic en **Siguiente**.
5. Si la tarea no se pudo ejecutar en el tiempo programado, puede elegir cuándo se ejecutará:
- **A la siguiente hora programada**
 - **Lo antes posible**
 - **Inmediatamente, si el tiempo desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el uso del selector **Tiempo desde la última ejecución**)

6. Haga clic en **Siguiente**. Según el tipo de tarea, podría ser necesario especificar los **Detalles de la tarea**. Una vez finalizado, haga clic en el botón **Terminar**. La nueva tarea programada aparecerá en la vista de [Tareas programadas](#).

3.8.1.5 Cómo programar una tarea de exploración (cada 24 horas)

Para programar una tarea habitual, vaya a **ESET Mail Security > Herramientas > Tareas programadas**. A continuación, se presenta una breve guía sobre cómo programar una tarea para explorar las unidades locales cada 24 horas.

Para programar una tarea de exploración:

1. Haga clic en **Agregar** en la pantalla principal de Tareas programadas.
2. Seleccione **Exploración del equipo a petición** en el menú desplegable.
3. Ingrese un nombre para la tarea y seleccione **Reiteradamente**.
4. Elija ejecutar la tarea cada 24 horas (1440 minutos).
5. Seleccione una acción para realizar en caso de que la ejecución de la tarea no se lleve a cabo por algún motivo.
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Destino**, seleccione Unidades locales.
8. Haga clic en **Finalizar** para aplicar la tarea.

3.8.1.6 Cómo quitar un virus del servidor

Si su equipo muestra síntomas de infección por malware; por ejemplo, si funciona más lento o con frecuencia no responde, se recomienda hacer lo siguiente:

1. Desde la ventana principal de ESET Mail Security, haga clic en **Exploración del equipo**.
2. Haga clic en **Exploración inteligente** para comenzar a explorar el sistema.
3. Una vez finalizada la exploración, consulte el registro con la cantidad de archivos explorados, infectados y desinfectados.
4. Si solo desea explorar una parte determinada del disco, elija **Exploración personalizada** y seleccione los objetos, para explorar en busca de virus.

Para obtener más información, consulte nuestro [artículo de la base de conocimiento de ESET](#), que se actualiza periódicamente.

3.8.2 Enviar una solicitud de soporte

Con el fin de proporcionar asistencia lo más rápido posible y con la mayor exactitud, ESET solicita la información sobre la configuración de ESET Mail Security, la información detallada sobre el sistema y los procesos activos ([Archivos de registro ESET SysInspector](#)) y los datos de registro. ESET usará estos datos únicamente para proporcionar asistencia técnica al cliente.

Cuando envía el formulario web, los datos de configuración de su sistema se enviarán a ESET. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Para enviar el formulario sin enviar los datos, haga clic en **No enviar datos**, y puede contactar a la atención al cliente de ESET mediante el formulario de soporte en línea.

Esta configuración también se puede establecer en **Configuración avanzada > Herramientas > Diagnóstico > Atención al cliente**.

i NOTA

Si decidió enviar los datos del sistema, debe completar y enviar el formulario web. De lo contrario, no se creará su comprobante y se perderán los datos de su sistema.

3.8.3 Limpiador especializado de ESET

El Limpiador especializado de ESET es una herramienta de eliminación de infecciones de malware comunes tales como Conficker, Sirefef o Necurs. Para obtener más información, visite este artículo de la [Base de conocimiento de ESET](#).

3.8.4 Acerca de ESET Mail Security

Esta ventana proporciona detalles sobre la versión instalada de ESET Mail Security y la lista de los módulos instalados del programa. El sector superior de la ventana incluye la información sobre el sistema operativo y los recursos del sistema.

Nombre del componente	Versión	Fecha de cre...
Base de datos de firmas de virus: 12149 (20150825)	12149	25-Aug-15
Módulo de respuesta rápida: 6569 (20150825)	6569	25-Aug-15
Módulo de actualización: 1060 (20150617)	1060	17-Jun-15
Módulo de exploración antivirus y antispyware: 1466 (20150813)	1466	13-Aug-15
Módulo de heurística avanzada: 1159 (20150820)	1159	20-Aug-15
Módulo de soporte de archivos comprimidos: 1235 (20150728)	1235	28-Jul-15

Puede copiar la información sobre los módulos (**Componentes instalados**) al portapapeles con un clic en **Copiar**. Puede resultar útil durante la solución de problemas o al ponerse en contacto con el soporte técnico.

3.8.5 Activación del producto

Luego de que la instalación se complete, se le solicitará que active el producto.


Hay varios métodos para activar su producto. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar según el país, así como de los medios de distribución (CD/DVD, página web de ESET, etc.).

Para activar su copia de ESET Mail Security directamente desde el programa, haga clic en el ícono de la bandeja del sistema y seleccione **El producto no está activado** del menú. También puede activar su producto desde el menú principal en **Ayuda y soporte > Activar el producto** o estado de **Seguimiento > El producto no está activado**.

Puede usar cualquiera de los siguientes métodos para activar ESET Mail Security:

- **Clave de licencia:** una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se usa para identificar al propietario de la licencia y para activarla.

- **Security Admin:** una cuenta creada en el [portal ESET License Administrator](#) con credenciales (dirección de correo electrónico + contraseña). Este método le permite administrar múltiples licencias desde una ubicación.
- Archivo de **Licencia sin conexión:** un archivo generado automáticamente que será transferido al producto de ESET para brindar información sobre la licencia. Su licencia sin conexión se genera desde el portal de licencias y se usa en los entornos donde la aplicación no puede conectarse con la autoridad otorgante.
- Haga clic en **Activar más tarde** con Remote Administrator de ESET si su equipo es miembro de una red administrada y su administrador realizará la activación remota a través de ESET Remote Administrator. Además, puede utilizar esta opción si desea activar este cliente más tarde.

Seleccione **Ayuda y soporte > Administrar licencia** en la ventana principal del programa para administrar la información de su licencia en cualquier momento. Verá la ID pública de la licencia usada por ESET para identificar su producto y para la identificación de la licencia. El nombre de usuario bajo el cual su equipo está registrado se almacena en la sección **Acerca de** que puede visualizar al hacer clic con el botón derecho en el icono de la bandeja del sistema .

NOTA

ESET Remote Administrator tiene la capacidad de activar equipos de clientes de manera silenciosa con el uso de licencias que el administrador pone a disposición.

3.8.5.1 Registro

Registre su licencia al completar los campos que se incluyen en el formulario de registro y haga clic en **Continuar**. Los campos marcados como requeridos entre paréntesis son obligatorios. Esta información solo se usará para cuestiones relacionadas con su licencia de ESET.

3.8.5.2 Activación de Security Admin

La cuenta de Security Admin es una cuenta creada en el portal de licencias con su **dirección de correo electrónico y contraseña**, que puede ver todas las autorizaciones para la instalación.

Una cuenta de **Security Admin** le permite administrar múltiples licencias. Si no posee una cuenta de Security Admin, haga clic en **Crear cuenta** y será redireccionado a la página web del Administrador de licencias de ESET donde se puede registrar con sus credenciales.

Si ha olvidado su contraseña, haga clic en **¿Olvidó su contraseña?** y será redireccionado al Portal comercial de ESET. Ingrese su dirección de correo electrónico y haga clic en **Enviar** para confirmar. Luego de ello, obtendrá un mensaje con instrucciones para restablecer su contraseña.

NOTA

para obtener más información sobre el uso del Administrador de licencias de ESET, consulte la Guía del usuario [Administrador de licencias de ESET](#).

3.8.5.3 Falla en la activación

Falló la activación de ESET Mail Security. Asegúrese de haber ingresado la **Clave de licencia** apropiada o haber adjuntado una **Licencia sin conexión**. Si tiene una **Licencia sin conexión** diferente, ingrésela nuevamente. Para verificar la clave de licencia que ingresó, haga clic en **volver a verificar la Clave de licencia** o en **comprar una nueva licencia**, y se lo redireccionará a nuestra página web, donde puede comprar una nueva licencia.

3.8.5.4 Licencia

Si elige la opción de activación Security Admin, se le pedirá que seleccione una licencia asociada a la cuenta que vaya a usarse para ESET Mail Security. Haga clic en **Activar** para continuar.

3.8.5.5 Progreso de la activación

ESET Mail Security se está activando, tenga paciencia. Esto puede llevar unos minutos.

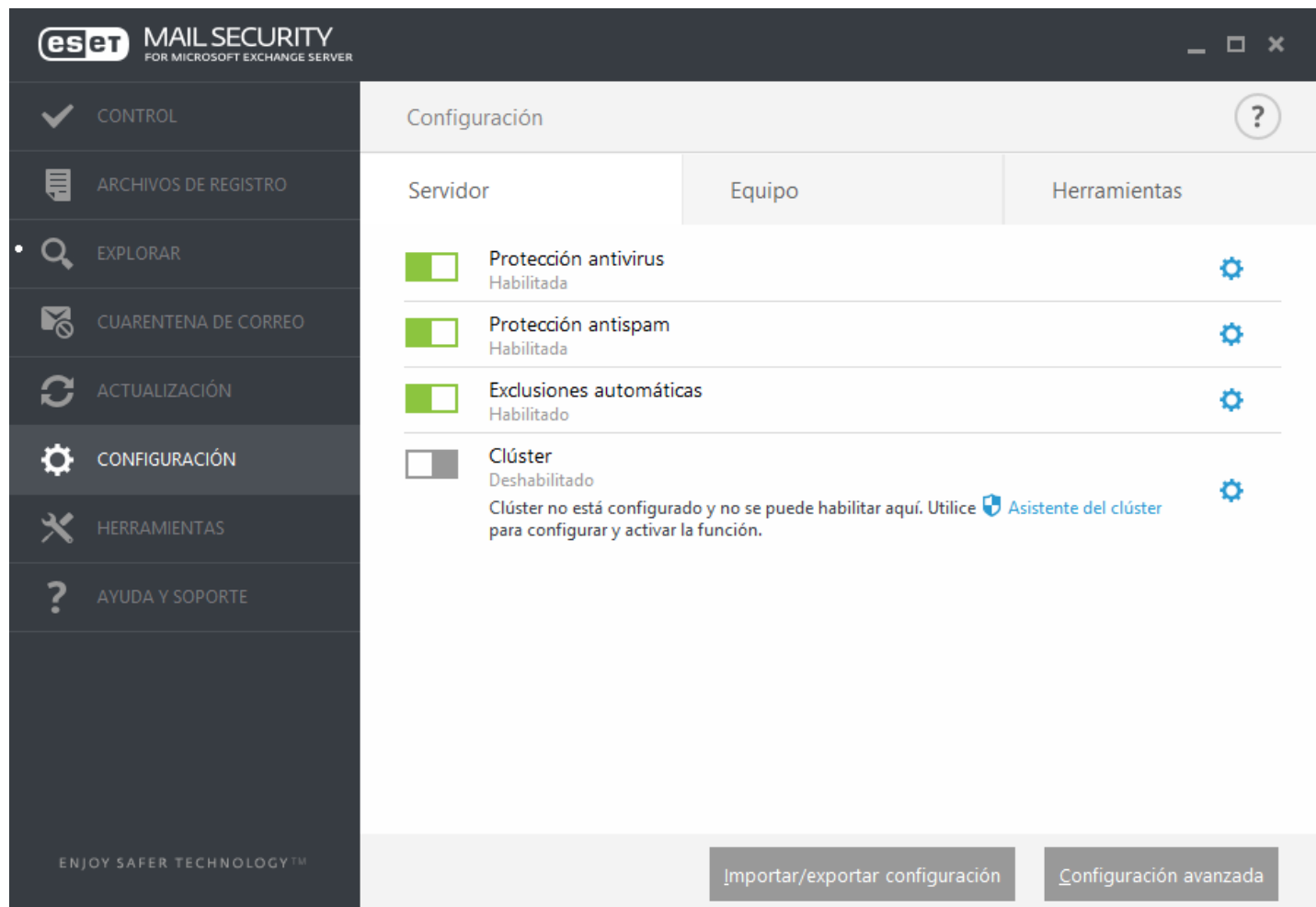
3.8.5.6 La activación se completó correctamente


La activación se completó correctamente y ESET Mail Security ahora está activado. A partir de este momento, ESET Mail Security recibirá actualizaciones regularmente para identificar las últimas amenazas y mantener su equipo seguro. Haga clic en **Listo** para finalizar con la activación del producto.


4. Trabajo con ESET Mail Security


El menú de **Configuración** contiene las siguientes secciones entre las cuales puede alternar mediante los tabuladores:

- [Servidor](#)
- [Equipo](#)
- [Herramientas](#)



Para deshabilitar temporalmente los módulos individuales, haga clic en el interruptor verde  junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del equipo.

Para volver a habilitar la protección de un componente de seguridad deshabilitado, haga clic en el interruptor rojo  para regresar un componente a su estado de habilitado.

Para acceder a configuraciones detalladas para un componente de seguridad específico, haga clic en la rueda de engranaje .

Haga clic en **Configuración avanzada** o presione **F5** para acceder a las configuraciones y opciones de los componentes adicionales.

Hay opciones adicionales en la parte inferior de la ventana de configuración. Para cargar los parámetros de configuración mediante un archivo de configuración *.xml* o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción **Importar/Exportar configuraciones**. Consulte [Importar/Exportar configuraciones](#) para obtener información más detallada.

4.1 Servidor

ESET Mail Security ofrece una protección significativa para Microsoft Exchange Server mediante las siguientes características:

- Antivirus y antispyware
- Protección antispam
- Reglas
- Protección del transporte de correo (Exchange Server 2007, 2010, 2013)
- Protección de la base de datos de correo electrónico (Exchange Server 2003, 2007, 2010)
- Exploración de la base de datos a petición (Exchange Server 2007, 2010, 2013)
- Cuarentena (configuraciones del tipo de cuarentena de correo electrónico)

Esta sección de configuración Avanzada le permite habilitar o deshabilitar la integración de la [Protección de la base de datos de correo electrónico](#) y la [Protección del transporte de correo](#) como también editar la [Prioridad del agente](#).

NOTA

si ejecuta Microsoft Exchange Server 2007 o 2010 puede elegir entre la Protección de la base de datos de correo electrónico y la Exploración de la base de datos a petición. No obstante, solo uno de estos dos tipos de protección puede estar activo a la vez. Si decide utilizar la Exploración de la base de datos a petición, deberá deshabilitar la integración de la Protección de la base de datos. De lo contrario, la [Exploración de la base de datos a petición](#) no estará disponible.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

INTEGRACIÓN

PROTECCIÓN DEL TRANSPORTE DE CORREO ELECTRÓNICO

Habilitar protección del transporte de correo

Configuración de prioridad de agentes

☒

Editar

Predeterminado

Aceptar

Cancelar

4.1.1 Configuración de la prioridad del agente

En el menú **Configuración de prioridad de agentes**, puede establecer la prioridad con la cual los agentes de ESET Mail Security se volverán activos después del inicio de Microsoft Exchange Server. El valor numérico define la prioridad. Cuanto menor sea el número, mayor será la prioridad. Esto aplica a Microsoft Exchange 2003.

Al seleccionar el botón **Editar** para ingresar la configuración de la prioridad del agente, puede establecer la prioridad con la cual se activarán los agentes de ESET Mail Security al iniciar Microsoft Exchange Server.

- **Modificar:** definir manualmente el número para cambiar la prioridad de un agente seleccionado.
- **Subir:** incrementa la prioridad del agente seleccionado moviéndolo hacia arriba en la lista de agentes.
- **Bajar:** disminuye la prioridad del agente seleccionado moviéndolo hacia abajo en la lista de agentes.

Con Microsoft Exchange Server 2003, puede especificar la prioridad del agente de manera independiente utilizando tabuladores para EOD (fin de la información) y RCPT (receptor).

4.1.1.1 Modificar prioridad

Si está ejecutando Microsoft Exchange Server 2003, puede definir el número de manera manual para cambiar la **Prioridad del agente de transporte**. Modifique el número en el campo de texto o utilice las flechas ascendente o descendente para cambiar la prioridad. Cuanto menor sea el número, mayor será la prioridad.

4.1.2 Configuración de la prioridad del agente

En el menú **Configuración de prioridad de agentes**, puede establecer la prioridad con la cual los agentes de ESET Mail Security se volverán activos después del inicio de Microsoft Exchange Server. Esto aplica a Microsoft Exchange 2007 y más reciente.

Configuración de prioridad de agentes

?

Nombre	Prioridad
Agente de filtrado de ESET	1
Agente de filtrado antivirus de ESET	2
Transport Rule Agent	3
Malware Agent	4
Text Messaging Routing Agent	5
Text Messaging Delivery Agent	6

Arriba

Abajo

Aceptar

- **Subir:** incrementa la prioridad del agente seleccionado moviéndolo hacia arriba en la lista de agentes.
- **Bajar:** disminuye la prioridad del agente seleccionado moviéndolo hacia abajo en la lista de agentes.

4.1.3 Antivirus y antispyware

En esta sección, puede configurar las opciones de **antivirus y antispyware** para su servidor de correo.

! IMPORTANTE

La protección del transporte de correo se proporciona mediante el agente de transporte y solo está disponible para Microsoft Exchange Server 2007 y posterior, pero su Exchange Server debe tener el rol de servidor Transporte Edge o el rol de servidor Transporte Hub. Esto también se aplica a una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor Transporte Edge o Hub).

Protección del transporte de correo electrónico:

Si deshabilita la opción **Habilitar la protección del transporte de correo para antivirus y antispyware**, el complemento de ESET Mail Security para Exchange Server no se sacará del proceso del servidor Microsoft Exchange. Solo pasará los mensajes sin explorarlos en busca de virus en la capa de transporte. Los mensajes se explorarán en busca de virus y spam en la capa de la base de datos del buzón de correo electrónico y se aplicarán las reglas existentes.

Configuración avanzada

SEVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

ANTIVIRUS Y ANTISPYWARE

PROTECCIÓN DEL TRANSPORTE DE CORREO ELECTRÓNICO

Habilitar protección antivirus y antispyware del transporte de correo

PARÁMETROS DE THREATSENSE

EXPLORACIÓN DE LA BASE DE DATOS A PETICIÓN

PARÁMETROS DE THREATSENSE

Predeterminado

Aceptar

Cancelar

Protección de la base de datos del buzón de correo electrónico:

Si deshabilita la opción **Habilitar la protección de la base de datos de correo electrónico para antivirus y antispyware**, el complemento de ESET Mail Security para Exchange Server no se sacará del proceso del servidor Microsoft Exchange. Solo pasará los mensajes sin explorarlos en busca de virus en la capa de la base de datos. Los mensajes se explorarán en busca de virus y spam en la capa de transporte y se aplicarán las reglas existentes.

Advanced setup

SERVER

Antivirus and antispamware

Antispam protection

Rules

Mail transport protection

Mailbox database protection

On-demand database scan

Quarantine

COMPUTER

UPDATE

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

ANTIVIRUS AND ANTISPYWARE

MAILBOX DATABASE PROTECTION

Enable antivirus and antispamware mailbox database protection

+

THREATSENSE PARAMETERS

MAIL TRANSPORT PROTECTION

Enable antivirus and antispamware mail transport protection

+

THREATSENSE PARAMETERS

ON-DEMAND DATABASE SCAN

+

THREATSENSE PARAMETERS

Default

OK

Cancel

4.1.4 Protección antispam

La protección antispam para su servidor de correo está habilitada en forma predeterminada. Para deshabilitarla, haga clic en el interruptor junto a **Habilitar protección antispam**.

NOTA

Deshabilitar la protección antispam no cambiará el [estado de protección](#). Aunque el antispam esté deshabilitado, verá **Protección máxima** en verde que aún se muestra en la sección de **Supervisión** de la GUI principal. Deshabilitar el Antispam no se considera una reducción en el nivel de protección.

Habilitar la función **Usar las listas blancas de Exchange Server para omitir automáticamente la protección antispam** permite a ESET Mail Security utilizar las “listas blancas” específicas de Exchange. Si esta opción está habilitada, se tendrá en cuenta lo siguiente:

- La dirección IP del servidor está en la lista de IP permitidas del Exchange Server
- El indicador Omitir antispam está configurado en el buzón de correo del destinatario del mensaje
- El destinatario del mensaje cuenta con la dirección del remitente en la lista Remitentes seguros (asegúrese de haber configurado la sincronización de la lista Remitentes seguros dentro del entorno del servidor de Exchange que incluye la Agregación de lista segura)

Si se aplica alguno de estos casos en un mensaje entrante, se omitirá la verificación antispam para este mensaje; por lo tanto, no se evaluará el mensaje en busca de SPAM y se enviará al buzón de correo del destinatario.

La función **Aceptar indicador de omisión de antispam configurado en la sesión SMTP** es útil cuando ha autenticado las sesiones de SMTP entre los servidores de Exchange con la configuración de omisión de antispam. Por ejemplo, cuando cuenta con un servidor Edge y un servidor Hub, no es necesaria la exploración del tráfico entre estos dos servidores. La función **Aceptar indicador de omisión de antispam configurado en la sesión SMTP** se habilita en forma predeterminada pero solo se aplica cuando el indicador de omisión de antispam esté configurado para la sesión SMTP en el servidor Exchange. Si deshabilita **Aceptar indicador de omisión de antispam configurado en la sesión SMTP**, ESET Mail Security explorará la sesión SMTP para detectar spam independientemente de la configuración de omisión de antispam del Exchange Server.

113

¡NOTA

es necesario actualizar con regularidad la base de datos del antispam para que el módulo antispam brinde la mejor protección posible. Para permitir las actualizaciones periódicas de la base de datos antispam, asegúrese de que ESET Mail Security tenga acceso a las direcciones IP correctas en los puertos necesarios. Para obtener más información sobre qué IP y puertos habilitar en el firewall de terceros, consulte el [artículo de KB](#).

4.1.4.1 Filtro y verificación

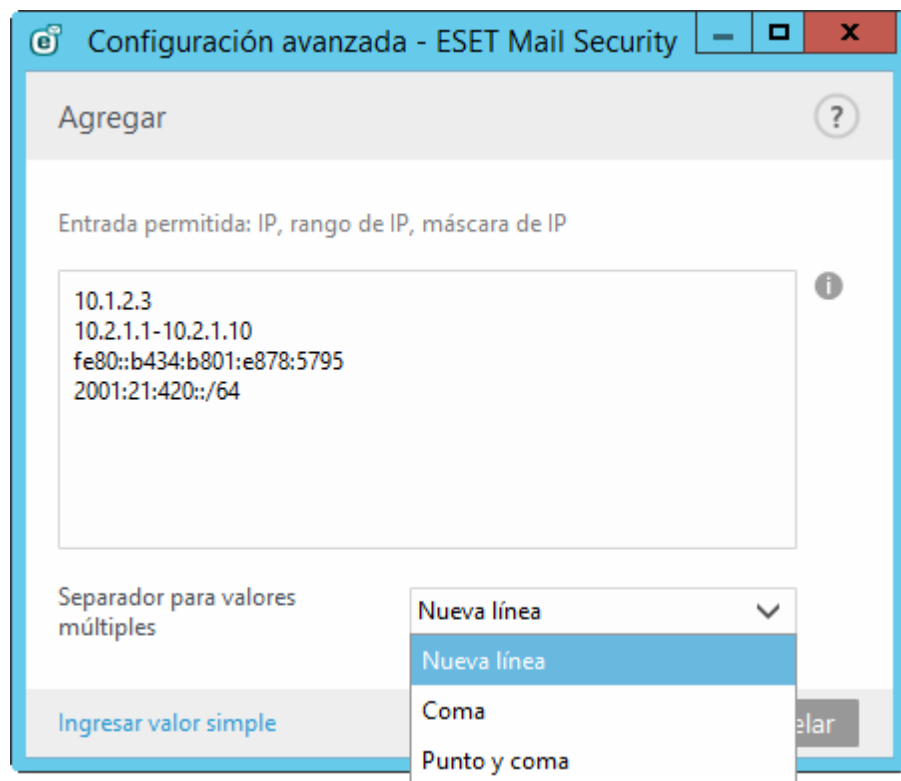
Puede configurar listas de **Permitidos**, **Bloqueados** e **Ignorados** al especificar criterios como la dirección o el rango IP, el nombre del dominio, etc. Para agregar, modificar o eliminar criterios, haga clic en **Editar** para abrir la lista que desea administrar.

- **Lista de IP aprobada:** coloca automáticamente en la lista blanca a los correos electrónicos que se originan desde direcciones IP especificadas.
- **Lista de IP bloqueada:** bloquea automáticamente los correos electrónicos que se originan desde direcciones IP especificadas.
- **Lista de IP ignorada:** lista de direcciones IP que serán ignoradas durante la clasificación.
- **Lista de dominios de remitentes bloqueados:** bloquea los mensajes de correo electrónico que contienen un dominio especificado en el cuerpo del mensaje.
- **Lista de dominios de remitentes ignorados:** los dominios especificados en el cuerpo del mensaje serán ignorados durante la clasificación.
- **Lista de IP de remitentes bloqueadas:** bloquea los mensajes de correo electrónico que contienen una dirección IP especificada en el cuerpo del mensaje.
- **Lista de IP de remitentes ignoradas:** las direcciones IP especificadas en el cuerpo del mensaje serán ignoradas durante la clasificación.
- **Lista de remitentes aprobados:** coloca en la lista blanca a los correos electrónicos que se originan desde un remitente especificado.
- **Lista de remitentes bloqueados:** bloquea los correos electrónicos que se originan desde un remitente especificado.
- **Lista de dominios a IP aprobados:** coloca en la lista blanca a los correos electrónicos que se originan desde direcciones IP que son resueltas desde dominios especificados en esta lista. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.
- **Lista de dominios a IP bloqueados:** bloquea los correos electrónicos que se originan desde direcciones IP que son resueltas desde dominios especificados en esta lista. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.
- **Lista de dominios a IP ignorados:** lista de dominios que se resuelve a direcciones IP que a la vez no serán verificadas durante la clasificación. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.
- **Lista de conjuntos de caracteres bloqueados:** bloquea correos electrónicos en conjuntos de caracteres especificados.
- **Lista de países bloqueados:** bloquea correos electrónicos de países especificados.

NOTA

Si desea agregar más entradas todas juntas, haga clic en **Ingresar valores múltiples** en la ventana emergente Agregar y seleccione el separador que debe utilizarse, puede ser **nueva línea**, **coma** o **punto y coma**.

Por ejemplo:



4.1.4.2 Configuración avanzada

Estas configuraciones permiten que los mensajes sean verificados por servidores externos (**RBL** - Listas de bloqueo en tiempo real, **DNSBL** - Lista de bloqueo DNS) según criterios definidos.

Número máximo de direcciones verificadas de Recibido: encabezados. - Puede limitar la cantidad de direcciones IP verificadas por antispam. Esto involucra las direcciones IP escritas en los encabezados de `Received: from`. El valor predeterminado es 0 que es sin límite.

Verificar la dirección del remitente con la lista negra de usuarios finales. los mensajes de correo electrónico que no se envían desde servidores de correo (equipos que no están en la lista de servidores de correo) se verifican para asegurarse de que el remitente no esté en la lista negra. Esta opción está activada de forma predeterminada. Puede desactivarla si es necesario, pero los mensajes no enviados desde servidores de correo no se verificarán con respecto a la lista negra.

Servidores RBL adicionales - Es una lista de servidores de Listas de bloqueo en tiempo real (RBL) que se consultan cuando se analizan los mensajes.

NOTA

Cuando agrega servidores RBL adicionales, ingrese el nombre de dominio del servidor (por ejemplo: `spamhaus.org`). Funcionará con cualquier código de devolución que sea compatible con el servidor.

Por ejemplo:

Agregar?

Entrada permitida: servidor o servidor:respuesta

spamhaus.org

i

Ingresar valores múltiples

Aceptar

Cancelar

Como alternativa, puede especificar un nombre de servidor con un código de devolución en la forma de `servidor:respuesta` (por ejemplo, `zen.spamhaus.org:127.0.0.4`). En este caso, recomendamos que agregue el nombre de cada servidor y el código de devolución de manera separada, para lograr una lista completa. Haga clic en **Ingresar valores múltiples** en la ventana emergente Agregar para especificar todos los nombres de servidores con sus códigos de retorno. Las entradas deben parecerse a este ejemplo, sus nombres reales de host de servidor RBL y códigos de retorno pueden variar:

Agregar?

Entrada permitida: servidor o servidor:respuesta

zen.spamhaus.org:127.0.0.2
zen.spamhaus.org:127.0.0.3
zen.spamhaus.org:127.0.0.4
spamhaus.org:127.0.1.2
spamhaus.org:127.0.1.3

i

Separador para valores múltiples

Nueva línea

▼

Ingresar valor simple

Aceptar

Cancelar

Límite de ejecución de la solicitud RBL (en segundos) - Esta opción permite que establezca un plazo máximo para las consultas RBL. Las respuestas RBL solo se usan desde aquellos servidores RBL que responden a tiempo. Si el valor está configurado en “0”, no se aplicará el tiempo de espera.

Número máximo de direcciones verificadas contra RBL - Esta opción le permite limitar la cantidad de direcciones IP que se consultan en el servidor RBL. Tenga en cuenta que la cantidad total de las consultas RBL será la cantidad de direcciones IP en el encabezado Recibido: (hasta una cantidad máxima de dirección IP en RBL) multiplicada por la cantidad de servidores RBL determinada en la lista RBL. Si el valor está configurado en "0", se verifica la cantidad ilimitada de encabezados recibidos. Tenga en cuenta que las direcciones IP que figuran en la lista de IP ignoradas no se cuentan para el límite de direcciones IP en RBL.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CONFIGURACIÓN AVANZADA

Número máximo de direcciones verificadas de Recibido: encabezados.

Verificar la dirección del remitente con la lista negra de usuarios finales.

Servidores RBL adicionales

RBL requiere un límite de ejecución (en segundos)

Número máximo de direcciones verificadas contra RBL

Servidores DNSBL adicionales

DNSBL requiere un límite de ejecución (en segundos)

Cantidad máxima de dominios verificados con DNSBL

Número máximo de dominios verificados contra DNSBL

Activar el registro de diagnóstico del motor

Predeterminado

Aceptar

Cancelar

Servidores DNSBL adicionales - Es una lista de servidores de Lista de bloqueo DNS (DNSBL) que se consultan con los dominios y las direcciones IP extraídos del cuerpo del mensaje.

NOTA
Cuando agrega servidores DNSBL adicionales, ingrese el nombre de dominio del servidor (por ejemplo: spamhaus.org). Funcionará con cualquier código de devolución que sea compatible con el servidor.

Por ejemplo:

Agregar

Entrada permitida: servidor o servidor:respuesta

spamhaus.org

Ingresar valores múltiples

Aceptar

Cancelar

Como alternativa, puede especificar un nombre de servidor con un código de devolución en la forma de servidor:respuesta (por ejemplo: zen.spamhaus.org:127.0.0.4). En este caso, recomendamos que agregue el

nombre de cada servidor y el código de devolución de manera separada, para lograr una lista completa. Haga clic en **Ingresar valores múltiples** en la ventana emergente Agregar para especificar todos los nombres de servidores con sus códigos de retorno. Las entradas deben parecerse a este ejemplo, sus nombres reales de host de servidor DNSBL y códigos de retorno pueden variar:

Agregar

?

Entrada permitida: servidor o servidor:respuesta

zen.spamhaus.org:127.0.0.2
zen.spamhaus.org:127.0.0.3
zen.spamhaus.org:127.0.0.4
spamhaus.org:127.0.1.2
spamhaus.org:127.0.1.3

i

Separador para valores múltiples

Nueva línea

▼

Ingresar valor simple

Aceptar

Cancelar

Límite de ejecución de la solicitud DNSBL (en segundos) - Le permite configurar un tiempo de espera máximo para todas las consultas DNSBL que deban completarse.

Número máximo de direcciones verificadas contra DNSBL - Le permite limitar la cantidad de direcciones IP que se consultan en el servidor de Lista de bloqueo DNS.

Número máximo de dominios verificados contra DNSBL - Le permite limitar la cantidad de dominios que se consultan en el servidor de Lista de bloqueo DNS.

Habilitar registro de diagnóstico del motor: registra información detallada acerca del motor Antispam en el archivo de registro con fines de diagnóstico. El motor Antispam no usa el registro de **Eventos** (archivo `warnlog.dat`) y, por lo tanto, no puede visualizar en el visor de [Archivos de registro](#). Escribe registros directamente en un archivo de texto dedicado (por ejemplo `C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log`) para que todos los datos de diagnóstico del motor Antispam se mantengan en un solo lugar. De esta manera, no se pone en peligro el desempeño de ESET Mail Security en caso de un enorme tráfico de correo electrónico.

Tamaño máximo de exploración de mensajes (kB) - Limita la exploración Antispam para los mensajes mayores al valor especificado. El motor de Antispam no explorará estos mensajes. Comportamiento:

Si el tamaño máximo de exploración de mensajes se establece en: 0 = exploración ilimitada

Si el tamaño máximo de mensajes se establece en: 1 - 12288 = 12288

Si el tamaño máximo de mensajes se establece en: más de 12 288 = establecer valor

Valor mínimo recomendado es 100kB.

Activar el rechazo temporal de los mensajes indeterminados: si el motor de correo no deseado no puede determinar si el mensaje es o no CORREO NO DESEADO, lo que significa que el mensaje tiene algunas características sospechosas de CORREO NO DESEADO pero no las suficientes para marcarlo como CORREO NO DESEADO (por ejemplo, el comienzo de una campaña o el origen de un rango IP con varias clasificaciones), esta configuración (cuando está habilitada) permite ESET Mail Security el rechazo temporal de dicho mensaje, de la misma manera que lo hacen las listas grises, y permite continuar con el rechazo durante un período específico, hasta:

a) el intervalo ha finalizado y el mensaje se aceptará en el siguiente intento de envío. El mensaje queda con la clasificación inicial (CORREO ELECTRÓNICO NO DESEADO o DESEADO).

b) La nube antispam recopila datos suficientes y puede clasificar correctamente el mensaje antes de que finalice el intervalo.

ESET Mail Security no guarda el mensaje rechazado ya que el servidor de correo lo debe volver a enviar según SMTP RFC.

Habilitar el envío de mensajes rechazados temporalmente para su análisis: el contenido del mensaje se envía automáticamente a los analistas para procesamiento e inspección manual. Esto ayuda a mejorar la clasificación de los mensajes de correo electrónico futuros.

! IMPORTANTE

Es posible que los mensajes rechazados temporalmente que se envíen para análisis sean en realidad mensajes DESEADOS. Por lo tanto, habilite esta característica solo si no hay riesgos de filtrar datos potencialmente sensibles.

4.1.4.3 Configuración de la lista gris

La función **Habilitar las listas grises** activa una característica que protege a los usuarios ante el spam mediante la siguiente técnica: El agente de transporte enviará un valor devuelto SMTP de “rechazo temporal” (el predeterminado es 451/4.7.1) por cualquier correo electrónico recibido que no pertenezca a un remitente conocido. Un servidor legítimo intentará volver a enviar el mensaje luego de un tiempo de espera. Por lo general, los servidores de spam no intentarán reenviar el mensaje, ya que hacen envíos a miles de direcciones de correo electrónico y no pierden tiempo reenviando el spam. La creación de listas grises es una capa adicional de protección antispam y no produce ningún efecto en la capacidad del módulo antispam para evaluar spam.

Al evaluar la fuente del mensaje, el método de creación de listas grises tiene en cuenta las listas de **Direcciones IP aprobadas**, **Direcciones IP ignoradas**, **Remitentes seguros** y **Permitir IP** en el servidor de Exchange, así como la configuración de la propiedad Omitir antispam para el buzón de correo del destinatario. Los correos electrónicos de estas listas de remitentes/direcciones IP o los distribuidos a un buzón de correo con la opción Omitir antispam habilitada, no serán examinados por el método de detección de listas grises.

Usar solo la parte de dominio de la dirección del remitente: ignora el nombre del receptor en la dirección de correo electrónico; solo tiene en cuenta el dominio.

Sincronizar las bases de datos de la lista gris sobre el clúster de ESET: las entradas de la base de datos de la lista gris se comparte en tiempo real entre los servidores del clúster de ESET. Cuando uno de los servidores recibe un mensaje que procesa la lista gris, esta información la difunde ESET Mail Security sobre el resto de los nodos en el clúster de ESET.

Límite de tiempo para la denegación de conexión inicial (min.): cuando se envía por primera vez un mensaje y se rechaza temporalmente, este parámetro define el período durante el cual siempre se rechazará el mensaje (determinado a partir del tiempo del primer rechazo). Cuando haya transcurrido el período definido, el mensaje se recibirá correctamente. El valor mínimo para ingresar es de 1 minuto.

Tiempo de vencimiento de las conexiones no verificadas (horas): este parámetro define el intervalo de tiempo mínimo para guardar el trío de datos. Un servidor válido debe reenviar un mensaje deseado antes de que transcurra este período. Este valor debe ser mayor que el valor del **Límite de tiempo para la denegación de conexión inicial**.

Tiempo de vencimiento de las conexiones verificadas (días): la cantidad mínima de días para guardar el trío de datos, durante la cual los correos electrónicos provenientes de un remitente específico se recibirán sin ninguna demora. Este valor debe ser mayor que el valor del **Tiempo de vencimiento de las conexiones no verificadas**.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CONFIGURACIÓN DE LA LISTA GRIS

Habilitar listado gris

Usar solo la parte de dominio de la dirección del remitente

Límite de tiempo para la denegación de la conexión inicial (min.)

Tiempo de vencimiento de las conexiones no verificadas (horas)

Tiempo de vencimiento de las conexiones verificadas (días)

Utilizar listas antispam para evadir automáticamente las listas grises

Lista blanca de IP

Lista blanca de dominios a IP

RESPUESTA SMTP

Código de respuesta

Código de estado

Predeterminado

Aceptar

Cancelar

Usar las lista de antispam para omitir automáticamente la lista gris: cuando está habilitada, se usa la lista de IP aprobado e ignorado junto con las listas blancas de IP para omitir automáticamente la lista gris.

Lista blanca de IP: en esta sección, puede agregar la dirección IP, dirección IP con máscara, intervalo IP. Puede modificar la lista haciendo clic en **Agregar**, **Editar** o **Quitar**. Como alternativa, puede **Importar** o **Exportar** los archivos. Use el botón de exploración ... para elegir la ubicación en el equipo para abrir o guardar el archivo de configuración.

Dominio para la lista blanca de IP: esta opción le permite especificar los dominios (por ejemplo *domainname.local*). Para gestionar la lista, use **Agregar** o **Quitar**.

Respuesta del SMTP (en el caso de las conexiones rechazadas temporalmente): puede especificar un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Ejemplo de un mensaje de respuesta de rechazo del SMTP:

Código de respuesta	Código de estado	Mensaje de respuesta
451	4.7.1	Inténtelo de nuevo más tarde

ADVERTENCIA
la sintaxis incorrecta en los códigos de respuesta SMTP puede provocar que la protección por listas grises no funcione correctamente. Como resultado, es posible que los mensajes de spam se envíen a los clientes o que directamente no se envíen.

NOTA
También puede usar variables del sistema para definir la respuesta de rechazo del SMTP.

4.1.4.4 SPF y DKIM

SPF (Marco de directiva del remitente) y **DKIM (Correo identificado con clave de dominio)** se utilizan como métodos de validación para comprobar que un mensaje de correo electrónico que asegura que proviene de un dominio específico está autorizado por el propietario de ese dominio. Esto ayuda a proteger a los destinatarios de recibir mensajes de correo electrónico falsificado.

La comprobación del **SPF** se lleva a cabo para verificar si un remitente legítimo envió el correo electrónico. Se realiza una búsqueda de DNS para los registros del SPF del dominio del remitente para obtener una lista de direcciones IP. Si alguna de las direcciones IP de los registros del SPF coincide con la dirección IP real del remitente, el resultado de la comprobación del SPF es **Aprobado**. Si la dirección IP real del remitente no coincide, el resultado es **Error**. Sin embargo, no todos los dominios tienen registros del SPF especificados en DNS. Si no existen registros del SPF en DNS, el resultado es **No disponible**. En ocasiones, se podría exceder el tiempo de espera de la solicitud DNS; en ese caso, el resultado también es **No disponible**.

DKIM se usa para evitar la suplantación de mensajes de correo electrónico al agregar una firma digital a los mensajes salientes según el estándar DKIM. Implica usar una clave de dominio privado para cifrar los encabezados de correo saliente del dominio y agregar una versión pública de la clave a los registros DNS del dominio. Los servidores del destinatario luego podrán recuperar la clave pública para descifrar los encabezados entrantes y verificar que el mensaje proviene realmente de su dominio y que no se ha cambiado en el camino.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CONFIGURACIÓN DE LA LISTA GRIS

SPF Y DKIM

Detectar servidores DNS automáticamente

☒

Dirección IP del servidor DNS

Tiempo de espera de la consulta de DNS (en segundos)

3

Rechazar mensajes automáticamente si falla la verificación de SPF

☐

Usar De: encabezado si CORREO DE está vacío

☐

Omitir automáticamente la lista gris si la verificación de SPF es correcta

☐

RESPUESTA DE RECHAZO DE SMTP

Código de respuesta

550

Código de estado

5.7.1

Mensaje de respuesta

SPF check failed

Predeterminado

Aceptar

Cancelar

Servidores DNS con autodetección: usa las configuraciones del adaptador de red.

Dirección IP del servidor DNS: si desea usar servidores DNS específicos para el SPF y DKIM, ingrese la dirección IP (en formato IPv4 o IPv6) del servidor DNS que desea usar.

Tiempo de espera de la consulta de DNS (segundos): especifica el tiempo de espera para la respuesta DNS.

Rechaza mensajes automáticamente si la comprobación del SPF es incorrecta: en caso de que el resultado de la comprobación del SPF sea incorrecta al comienzo, se puede rechazar el mensaje de correo electrónico antes de la descarga.

Use desde: encabezado si el correo del destinatario está vacío: el encabezado MAIL FROM puede estar vacío, también se puede falsificar fácilmente. Cuando esta opción está habilitada y la DIRECCIÓN DE CORREO DEL REMITENTE está vacía, el mensaje se descarga y en su lugar se usa el encabezado *From*.

Omitir automáticamente la lista gris si la comprobación del SPF está aprobada: no existe motivo para usar la lista gris para los mensajes que aprobaron la comprobación del SPF.

Respuesta de rechazo del SMTP: especifica un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Puede ingresar un mensaje de respuesta con el siguiente formato:

Código de respuesta	Código de estado	Mensaje de respuesta
550	5.7.1	Comprobación del SPF incorrecta

4.1.5 Reglas

Las **Reglas** permiten a los administradores definir manualmente las condiciones de filtrado de correo electrónico y las acciones que se deben realizar con los mensajes de correo electrónico filtrados.

Existen tres conjuntos de reglas independientes. Las reglas disponibles en su sistema dependen de la versión de Microsoft Exchange Server que tenga instalada en el servidor con ESET Mail Security:

- [Protección de la base de datos de correo electrónico](#): este tipo de protección solo está disponible para Microsoft Exchange Server 2010, 2007 y 2003 que funcionan en el rol de Servidor de casilla de correo (Microsoft Exchange 2010 y 2007) o Servidor de respaldo (Microsoft Exchange 2003). Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya el rol de Casilla de correo o Respaldo).
- [Protección del transporte de correo](#): esta protección es proporcionada por el agente de transporte y solo está disponible para Microsoft Exchange Server 2007 o más reciente que funcione en el rol de servidor Transporte Edge o servidor Transporte Hub. Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados).
- [Exploración de la base de datos a petición](#): le permite ejecutar o programar una exploración de la base de datos del buzón de correo Exchange. Esta característica solo está disponible para Microsoft Exchange Server 2007 o más reciente que funcione en el rol de Servidor de la casilla de correo o Transporte Hub. Esto también se aplica a una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados). Consulte [roles de Exchange Server 2013](#) para conocer algunos aspectos específicos acerca de los roles en Exchange 2013.

4.1.5.1 Lista de reglas

La ventana de la lista Las **reglas** muestra las reglas existentes. Las reglas se clasifican en tres niveles y se evalúan en este orden:

- **Reglas de filtrado (1)**
- **Reglas de procesamiento de adjuntos (2)**
- **Reglas de procesamiento de resultados (3)**

Las reglas que tienen el mismo nivel son evaluadas en el mismo orden en el cual se muestran en la ventana de Reglas. Solo puede cambiar el orden de la regla en el caso de las reglas que tienen el mismo nivel. Por ejemplo, cuando tiene múltiples reglas de filtrado, puede cambiar el orden en el cual se aplican. No puede cambiar su orden al colocar reglas de Procesamiento de adjuntos antes de las reglas de Filtrado, los botones Arriba/Abajo no estarán disponibles. En otras palabras, no puede mezclar las reglas de distintos Niveles.

IMPORTANTE

Normalmente, si se cumplen las condiciones de una regla, se detiene la evaluación de reglas para aplicar otras

reglas con menor prioridad. Sin embargo, si es necesario, puede usar una [Acción de regla](#) especial denominada **Evaluar otras reglas** para permitir que continúe la evaluación.

La columna Aciertos muestra la cantidad de veces que se aplicó con éxito la regla. Al anular la selección de una casilla de verificación (a la izquierda de cada nombre de regla) desactiva la regla correspondiente hasta seleccionar otra vez la casilla de verificación.

- **Agregar...** : agrega una nueva regla
- **Editar...** : modifica una regla existente
- **Quitar**: quita una regla seleccionada
- **Subir**: mueve la regla seleccionada hacia arriba en la lista
- **Bajar**: mueve la regla seleccionada hacia abajo en la lista
- **Restablecer**: restablece el contador para la regla seleccionada (la columna de Aciertos)

i NOTA

si se agregó una nueva regla o se modificó una regla existente, se iniciará en forma automática una nueva exploración de los mensajes usando las reglas nuevas o modificadas.

Las reglas se verifican con respecto a un mensaje cuando el agente de transporte o la interfaz VSAPI lo procesan. Si tanto el agente de transporte como VSAPI están habilitados y el mensaje concuerda con las condiciones de la regla, el contador de la regla puede incrementarse en dos o más puntos. Esto se debe a que VSAPI accede al cuerpo y al adjunto de un mensaje por separado, de modo que las reglas se aplican a cada parte de manera individual. Las reglas también se aplican durante la exploración en segundo plano (por ejemplo, cuando ESET Mail Security realiza una exploración del buzón de correo después de descargar una nueva base de datos de firmas de virus), lo que puede aumentar el contador de la regla (coincidencia).

4.1.5.1.1 Asistente de reglas

Puede definir las **Condiciones** y las **Acciones** mediante el asistente de **Reglas**. Defina primero las Condiciones, luego las Acciones.

- Haga clic en **Añadir** y aparecerá una ventana de [Condición de regla](#) donde podrá seleccionar el tipo de condición, la operación y el valor.
- Desde aquí puede añadir una [Acción de regla](#).
- Una vez que se definieron las condiciones y las acciones, ingrese un **Nombre** para la regla (algo que le permita reconocer a la regla), este nombre se mostrará en la [Lista de reglas](#).
- Si desea preparar reglas pero planea utilizarlas más tarde, puede hacer clic en el interruptor junto a **Activa** para desactivar la regla. Para activar la regla, seleccione la casilla de verificación junto a la regla que desea activar desde la [Lista de reglas](#).

i NOTA

Nombre es un campo obligatorio, si está resaltado en rojo, escriba el nombre de la regla en el cuadro de texto y haga clic en el botón **Aceptar** para crear la regla. El resaltado en rojo no desaparece aunque haya ingresado el nombre de la regla, solo desaparece después de que haga clic en **Aceptar**.

Algunas **Condiciones** y **Acciones** difieren en el caso de las reglas específicas para **Protección del transporte de correo**, **Protección de la base de datos de correo electrónico** y **Exploración de la base de datos a petición**. Esto se debe a que cada uno de estos tipos de protección utiliza un enfoque un poco distinto para procesar los mensajes, especialmente la **Protección del transporte de correo**.

! IMPORTANTE

Si define varias condiciones, se debe cumplir con todas las condiciones para aplicar la regla. Todas las condiciones se conectan mediante el operador lógico AND [Y]. Incluso si se cumple con la mayoría de las condiciones y solo uno no la cumple, el resultado de la evaluación de condiciones se considera *no cumplido* y no se puede adoptar la acción de la regla.

Regla



Activo

☒

Nombre

Tipo de condición	Operación	Parámetros

Agregar

Editar

Quitar

Tipo de acción	Parámetro

Agregar

Editar

Quitar

Aceptar

Cancelar

i NOTA

Si configura el tipo de acción **Eventos de registro** para la protección de la base de datos del buzón de correo con el parámetro %IPAddress%, la columna **Evento** en los [archivos de registro](#) estará vacía para este evento particular. Esto se debe a que no hay dirección de IP en el nivel de protección de base de datos del buzón de correo. Algunas opciones no están disponibles en todos los niveles de protección:

Dirección de IP: ignorada por la **exploración de base de datos bajo demanda y protección de base de datos del buzón de correo**

Buzón de correo:- ignorado por la **Protección del transporte de correo electrónico**

4.1.5.1.1.1 Condición de regla

Este asistente le permite añadir condiciones para una regla. Seleccione **Tipo > Operación** en la lista desplegable (la lista de operaciones cambia según la regla que haya elegido) y seleccione **Parámetro**. Los campos del Parámetro cambiarán según el tipo de regla y la operación.

Por ejemplo, elija **El tamaño del adjunto > es mayor a** y en **Parámetro** especifique 10 MB. Al utilizar estas configuraciones, cualquier mensaje que contenga un adjunto mayor a 10 MB será procesado mediante la [acción](#) de regla que haya especificado. Por este motivo debe especificar la acción que se tomará cuando se active una regla determinada, si aún no lo hizo cuando configuró los parámetros para esa regla.

i NOTA

Es posible añadir varias condiciones para una regla.

Las siguientes condiciones están disponibles para la **Protección de transporte de correo electrónico**, **Protección de la base de datos del buzón de correo electrónico** y **Exploración de la base de datos a petición** (no se mostrarán algunas de las opciones según las condiciones seleccionadas anteriormente):

Nombre de las condiciones	Protección del transporte de correo electrónico	Protección de la base de datos del buzón de correo electrónico	Exploración de la base de datos a petición	Descripciones
Asunto	✓	✓	✓	Se aplica a los mensajes que contengan o no una cadena específica (o una expresión habitual) en el asunto.
Remitente	✓	✓	✓	Se aplica a los mensajes enviados por un remitente específico.
Dirección IP del remitente	✓	✗	✗	Se aplica a los mensajes enviados desde una dirección IP específica.
Dominio del remitente	✓	✓	✓	Se aplica a los mensajes de un remitente con un dominio específico en la dirección de correo electrónico.
Destinatario	✓	✓	✓	Se aplica a los mensajes enviados a un destinatario específico.
Unidades organizativas del destinatario	✓	✗	✗	Se aplica a los mensajes enviados a un destinatario de una unidad organizativa específica.
Resultado de validación del destinatario	✓	✗	✗	Se aplica a los mensajes enviados a un destinatario validado en Active Directory.
Nombre del archivo adjunto	✓	✓	✓	Se aplica a los mensajes que contienen datos adjuntos con un nombre específico.
Tamaño de los datos adjuntos	✓	✓	✓	Se aplica a los mensajes que tengan datos adjuntos que no cumplan con un tamaño específico, que se encuentren dentro de un rango de tamaño específico o que superen un tamaño específico.
Tipo de datos adjuntos	✓	✓	✓	Se aplica a los mensajes que tienen tipo de archivo específico adjunto. Los tipos de archivos se categorizan en grupos para facilitar la selección, puede seleccionar varios tipos de archivos o categorías completas.
Tamaño del mensaje	✓	✗	✗	Se aplica a los mensajes que tengan datos adjuntos que no cumplan con un tamaño específico, que se encuentren dentro de un rango de tamaño específico o que superen un tamaño específico.
Buzón de correo	✗	✓	✗	Se aplica a los mensajes ubicados en un buzón de correo específico.
Encabezados del mensaje	✓	✓	✗	Se aplica a los mensajes que tienen datos específicos presentes en el encabezado del mensaje.
Resultado de la exploración antispam	✓	✗	✗	Se aplica a los mensajes marcados como Ham o Spam.
Resultado de la exploración antivirus	✓	✓	✓	Se aplica a los mensajes marcados como malintencionados o no.

Nombre de las condiciones	Protección del transporte de correo electrónico	Protección de la base de datos del buzón de correo electrónico	Exploración de la base de datos a petición	Descripciones
Mensaje interno	✓	✗	✗	Se aplica según si el mensaje es interno o externo.
Tiempo de recepción	✓	✓	✓	Se aplica a los mensajes recibidos antes o después de una fecha específica o durante un rango de fechas específico.
Contiene un archivo protegido por contraseña	✓	✓	✓	Se aplica a los mensajes con datos adjuntos que están protegidos por contraseña.
Contiene un archivo dañado	✓	✓	✓	Se aplica a los mensajes que tienen datos adjuntos que están dañados (probablemente será imposible abrirlos).
Resultado de DKIM	✓	✗	✗	Se aplica a los mensajes que aprobaron o reprobaron la verificación de DKIM, de manera alternativa si no está disponible.
Resultado de SPF	✓	✗	✗	Se aplica a los mensajes que aprobaron o reprobaron la verificación de SPF, de manera alternativa si no está disponible.
Resultado de DMARC	✓	✗	✗	Se aplica a los mensajes que aprobaron o reprobaron la verificación de SPF, DKIM o ambas, de manera alternativa si no está disponible.

4.1.5.1.1.2 Acción de regla

Puede añadir acciones que se tomarán con mensajes o adjuntos que coincidan con las condiciones de las reglas.

i NOTA

Es posible añadir varias condiciones para una regla.

La lista de **Acciones** disponibles para la **Protección del transporte de correo**, **Protección de la base de datos del buzón de correo** y la **Exploración de la base de datos a petición** (es posible que algunas de las opciones no se muestren según las condiciones seleccionadas):

Nombre de las acciones	Protección del transporte de correo electrónico	Protección de la base de datos del buzón de correo electrónico	Exploración de la base de datos a petición	Descripciones
Mensaje en cuarentena	✓	✗	✗	El mensaje no se entregará al destinatario y se moverá a la cuarentena de correo .
Colocar el archivo adjunto en cuarentena	✓	✓	✓	Coloca los datos adjuntos del correo electrónico en archivo en cuarentena , el correo electrónico se entregará al destinatario con los datos adjuntos truncados a longitud cero.
Eliminar adjunto	✓	✓	✓	Elimina los datos adjuntos del mensaje; el mensaje se entregará al destinatario sin los datos adjuntos.

Nombre de las acciones	Protección del transporte de correo electrónico	Protección de la base de datos del buzón de correo electrónico	Exploración de la base de datos a petición	Descripciones
Rechazar mensaje	✓	✗	✗	El mensaje no se entregará y se enviará un NDR (Informe de no entrega) al remitente.
Eliminar el mensaje en silencio	✓	✗	✗	Elimina un mensaje sin enviar un informe de no entrega.
Establecer el valor SCL	✓	✗	✗	Cambia o establece un valor SCL específico.
Enviar notificación por correo electrónico	✓	✓	✓	Envía notificaciones de correo electrónico a un destinatario específico en las Notificaciones de correo electrónico . Necesita habilitar la característica Enviar notificación de evento por correo electrónico . Entonces puede personalizar el formato de los mensajes de evento (use la información sobre herramientas para obtener las sugerencias) mientras crea la regla. Además, puede seleccionar el nivel de detalle para los mensajes de evento, aunque esto depende de la configuración de nivel de detalle mínima en la sección Notificaciones de correo electrónico .
Omitir la exploración antispam	✓	✗	✗	El motor antispam no explorará el mensaje.
Omitir la exploración antivirus	✓	✓	✓	El motor antivirus no explorará el mensaje.
Evaluar otras reglas	✓	✓	✓	Permite la evaluación de otras reglas, habilita al usuario a definir varios grupos de condiciones y varias acciones a seguir, según las condiciones.
Registrar eventos	✓	✓	✓	Escribe la información acerca de la regla aplicada al registro de programa y define el formato de los mensajes de evento (use información sobre herramientas para obtener más sugerencias).
Agregar campo de encabezado	✓	✗	✗	Agrega una cadena personalizada al encabezado del mensaje.
Reemplazar adjunto con información sobre la acción	✗	✓	✓	Quita los datos adjuntos y agrega información acerca de la acción tomada con los datos adjuntos para el cuerpo del mensaje.
Eliminar mensaje	✗	✓	✓	Elimina el mensaje infectado.
Mover el mensaje a la papelera	✗	✗	✓	Coloca un mensaje de correo electrónico en la papelera en el lado del cliente de correo electrónico.
Aplicar la política de DMARC	✓	✗	✗	Si se cumple con la condición del resultado DMARC, el mensaje de correo electrónico se gestiona según la política especificada en el registro DMARC DNS del dominio del remitente.

4.1.6 Protección del transporte de correo electrónico

Los siguientes sistemas tienen la **Protección del transporte de correo electrónico** disponible en **Configuraciones avanzadas > Servidor**:

- Microsoft Exchange Server 2003 (Servidor Front-end)
- Microsoft Exchange Server 2003 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2007 (Rol del servidor de Transporte Edge o Transporte Hub)
- Microsoft Exchange Server 2007 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2010 (Rol del servidor de Transporte Edge o Transporte Hub)
- Microsoft Exchange Server 2010 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2013 (rol de servidor Transporte Edge)
- Microsoft Exchange Server 2013 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2016 (rol de servidor Transporte Edge)
- Microsoft Exchange Server 2016 (rol de servidor de buzón de correo)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

La acción del antivirus sobre la capa de transporte puede configurarse en **Acción para realizar cuando no es posible desinfectar**:

- **Sin acción**: conservar los mensajes infectados que no pueden desinfectarse
- **Poner el mensaje en cuarentena**: enviar los mensajes infectados a la cuarentena del buzón de correo
- **Eliminar el mensaje**: eliminar el mensaje infectado
- **Abandonar mensaje en silencio**: elimina los mensajes sin enviar NDR (Informe de no entrega)

NOTA

Si selecciona **Sin acción** y al mismo tiempo tiene el **Nivel de limpieza** ajustado a **Sin limpieza** en los [parámetros de ThreatSense](#) del [antivirus y antispyware](#), entonces el [estado de protección](#) cambiará a amarillo. Es porque es un riesgo de seguridad y no recomendamos usar esta combinación. Cambie una u otra configuración para obtener un buen nivel de protección.

La acción antispam sobre la capa de transporte puede configurarse en **Acción para los mensajes de spam**:

- **Sin acción**: conservar el mensaje aunque esté marcado como spam
- **Poner el mensaje en cuarentena**: envía los mensajes marcados como spam a la cuarentena del buzón de correo
- **Rechazar mensaje**: rechazar los mensajes marcados como spam
- **Abandonar mensaje en silencio**: elimina los mensajes sin enviar NDR (Informe de no entrega)

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

PROTECCIÓN DEL TRANSPORTE DE CORREO ELECTRÓNICO

Acción para emprender si no es posible la desinfección

Rechazar mensaje

Acción a realizar en el mensaje spam

Sin acción

Mensaje de cuarentena

Rechazar mensaje

Omitir el mensaje en silencio

RESPUESTA DE RECHAZO DE SMTP

Código de respuesta

554

Código de estado

5.6.0

Mensaje de respuesta

Invalid content

Escribir los resultados de la exploración en los encabezados de mensajes

☒

Agregar notificación al cuerpo de los mensajes explorados

Solo adjuntar a los mensajes in...

Agregar nota al asunto de los mensajes infectados:

☒

Plantilla añadida al asunto de los mensajes infectados

[found threat %VIRUSNAME%]

Añadir una nota al asunto de los mensajes spam

☒

Predeterminado

Aceptar

Cancelar

Respuesta de rechazo SMTP: puede especificar un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Puede ingresar un mensaje de respuesta con el siguiente formato:

Código de respuesta	Código de estado	Mensaje de respuesta
250	2.5.0	Se aceptó y completó la acción solicitada para el correo
451	4.5.1	Se anuló la acción solicitada: error local de procesamiento
550	5.5.0	No se ejecutó la acción solicitada: buzón de correo no disponible
554	5.6.0	Contenido no válido

NOTA

cuando configure las respuestas SMTP de rechazo, también puede utilizar variables del sistema.

Escribir los resultados de la exploración en los encabezados de mensajes: cuando está habilitado, los resultados de una exploración se escriben en los encabezados de los mensajes. Estos encabezados de mensajes comienzan con `X_ESET` lo que facilita reconocerlos (por ejemplo `X_EsetResult` o `X_ESET_Antispam`).

Agregar notificación al cuerpo de los mensajes escaneados ofrece tres opciones:

- No adjuntar a los mensajes
- Solo adjuntar a los mensajes infectados
- Añadir a todos los mensajes explorados (no aplica para mensajes internos)

Agregar una nota al asunto de los mensajes infectados: cuando está habilitado, ESET Mail Security añadirá una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes infectados** (el texto predeterminado por defecto es `[found threat %VIRUSNAME%]`). Esta

129

modificación puede utilizarse para automatizar el filtrado de mensajes infectados al filtrar correos electrónicos que tengan un asunto específico, por ejemplo, al utilizar las [reglas](#) o de manera alternativa del lado del cliente (si el cliente de correo electrónico lo admite) para colocar dichos mensajes de correo electrónico en una carpeta aparte.

Agregar una nota al asunto de los mensajes de spam: cuando ESET Mail Security está habilitado, añadirá una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes de spam** (texto predeterminado por defecto [SPAM]). Esta modificación puede utilizarse para automatizar el filtrado de spam al filtrar correos electrónicos que tengan un asunto específico, por ejemplo, al utilizar las [reglas](#) o de manera alternativa del lado del cliente (si el cliente de correo electrónico lo admite) para colocar dichos mensajes de correo electrónico en una carpeta aparte.

i NOTA

también puede utilizar las variables del sistema cuando edita texto, que serán añadidas al asunto.

4.1.6.1 Configuración avanzada

En esta sección puede cambiar las configuraciones avanzadas que se aplican al agente de transporte:

- **Explorar también los mensajes procedentes de conexiones autenticadas o internas:** puede seleccionar qué tipo de escaneo realizar a mensajes recibidos desde fuentes autenticadas o servidores locales. Se recomienda el escaneo de dichos mensajes ya que aumenta la protección, pero son necesarios si utiliza el conector POP3 incorporado de Microsoft SBS para obtener mensajes de correo electrónico desde servidores POP3 o servicios de correo externos (por ejemplo **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem**, etc.). Para obtener más información, consulte [Conector POP3 y antispam](#).

i NOTA

Esta configuración enciende o apaga la **Protección antispam** para los usuarios autenticados y las conexiones internas. Enciende y apaga la **Protección antivirus** para las conexiones autenticadas. Sin embargo, los correos electrónicos de conexiones no autenticadas siempre se exploran con el **Antivirus**, incluso si ha seleccionado **No explorar**.

i NOTA

Los mensajes internos de Outlook dentro de la organización se envían en formato TNEF (Transport Neutral Encapsulation Format). El formato TNEF no es compatible con antispam. Por lo tanto, los correos electrónicos internos con formato TNEF no se explorarán en busca de spam aunque haya seleccionado **Explorar con la protección antispam** o **Explorar con la protección antivirus y antispam**.

- **Buscar la dirección IP inicial en los encabezados:** si se habilita esta opción, ESET Mail Security busca la dirección IP que se origina en los encabezados de mensajes para que los diferentes módulos de protección (Antispam y demás) puedan utilizarla. En caso de que su Organización Exchange se encuentre separada de Internet mediante un Proxy, una Puerta de enlace o un servidor Transporte perimetral, los mensajes por correo electrónico parecen provenir desde una dirección IP individual (generalmente una interior). Es común que uno de los servidores exteriores (por ejemplo Transporte Edge en DMZ), donde se conoce la dirección IP del remitente, esta dirección IP esté escrita dentro de los encabezados de correo que se reciben. El valor especificado en el campo **Encabezado con la IP inicial** debajo es el encabezado que ESET Mail Security busca en un encabezado de mensaje.
- **Encabezado con la IP inicial:** es el encabezado que ESET Mail Security busca en los encabezados de correo. Por lo general, es **X-Originating-IP**, pero puede ingresar otros encabezados estándar de la industria tales como **X-Forwarded-For** o **Forwarded** (consulte la lista [campos de encabezado HTTP](#)).
- **Activar cuarentena de los mensajes internos:** cuando esta opción está habilitada, se colocarán los mensajes en cuarentena. Por lo general no hay necesidad de poner los mensajes internos en cuarentena; sin embargo, si lo requiere, puede activarla.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

+

PROTECCIÓN DEL TRANSPORTE DE CORREO ELECTRÓNICO

↩

-

CONFIGURACIÓN AVANZADA

↩

Explorar también los mensajes recibidos de conexiones autenticadas o internas

Explorar con la protección antivirus y antispyware

Buscar la dirección IP inicial en los encabezados

Explorar con la protección antivirus

Encabezado con la IP inicial

Explorar con la protección antispam

Activar cuarentena de los mensajes internos

Explorar con la protección antivirus y antispyware

Predeterminado

Aceptar

Cancelar

4.1.7 Protección de la base de datos del buzón de correo electrónico

Los siguientes sistemas operativos tienen la **Protección de la base de datos de correo electrónico** disponible en **Configuraciones avanzadas > Servidor**:

- Microsoft Exchange Server 2003 (Servidor Back-end)
- Microsoft Exchange Server 2003 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2007 (rol de servidor de buzón de correo)
- Microsoft Exchange Server 2007 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2010 (rol de servidor de buzón de correo)
- Microsoft Exchange Server 2010 (instalación de servidor único con roles múltiples)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

i NOTA

La protección de la base de datos del buzón de correo electrónico no está disponible para Microsoft Exchange Server 2013 y 2016.

Si anula la selección de la opción **Habilitar la protección antivirus y antispyware VSAPI 2.6**, el complemento de ESET Mail Security para Exchange Server no se sacará del proceso de Microsoft Exchange Server. Solo pasará los mensajes sin explorarlos en busca de virus. Sin embargo, se explorarán los mensajes en busca de [spam](#) y se aplicarán las [reglas](#).

Si la opción **Exploración proactiva** está habilitada, los nuevos mensajes entrantes se explorarán en el mismo orden en que fueron recibidos. Cuando esta opción está habilitada y un usuario abre un mensaje aún no explorado, dicho mensaje se explorará antes que los demás mensajes de la cola de espera.

Exploración en segundo plano permite que la exploración de todos los mensajes se ejecute en segundo plano (la exploración se ejecuta en la casilla de correo y la tienda de carpetas públicas, por ejemplo, la base de datos de Exchange). Microsoft Exchange Server decide si una exploración en segundo plano se ejecutará o no basándose en diversos factores, como la carga actual del sistema, la cantidad de usuarios activos, etc. Microsoft Exchange Server lleva un registro de los mensajes explorados y de la versión de la base de datos de firmas de virus utilizada. Si abre un mensaje que no se exploró con la base de datos de firmas de virus más reciente, Microsoft Exchange Server envía el mensaje a ESET Mail Security para su exploración antes de que lo abra el cliente de correo electrónico. Puede elegir **Explorar solo los mensajes que contienen archivos adjuntos** y filtrarlos según el momento en que se recibieron, mediante las siguientes opciones de **Nivel de exploración**:

- **Todos los mensajes**
- **Mensajes recibidos en el último año**
- **Mensajes recibidos en los últimos 6 meses**
- **Mensajes recibidos en los últimos 3 meses**
- **Mensajes recibidos en el último mes**
- **Mensajes recibidos en la última semana**

Como la exploración en segundo plano puede afectar la carga del sistema (la exploración se realiza luego de cada actualización de la base de datos de firmas de virus), es recomendable programar las exploraciones fuera de las horas laborales. La exploración en segundo plano programada se puede configurar mediante la creación de una tarea especial en la sección de Tareas programadas. Cuando programa una tarea de exploración en segundo plano, puede especificar la hora de inicio, la cantidad de repeticiones y otros parámetros disponibles en las Tareas programadas. Luego de haber programado la tarea, ésta aparecerá en la lista de tareas programadas y será posible modificar sus parámetros, eliminarlas o desactivarla temporalmente.

Al habilitar la opción **Explorar el cuerpo de los mensajes RTF**, se activa la exploración del cuerpo de los mensajes RTF. El cuerpo de los mensajes RTF pueden contener virus de macro.

i NOTA

VSAPI no explora el cuerpo de los correos electrónicos cuyo texto no tiene formato.

i NOTA

las carpetas públicas se tratan de la misma manera que los buzones de correo. Esto implica que las carpetas públicas también son exploradas.

4.1.8 Exploración de la base de datos a petición

Lista de sistemas que tienen disponible la **Exploración de la base de datos a petición**:

- Microsoft Exchange Server 2007 (rol de servidor del buzón de correo o Transporte Hub)
- Microsoft Exchange Server 2007 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2010 (rol de servidor del buzón de correo o Transporte Hub)
- Microsoft Exchange Server 2010 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2013 (rol de servidor de buzón de correo)
- Microsoft Exchange Server 2013 (instalación de servidor único con roles múltiples)
- Microsoft Exchange Server 2016 (rol de servidor de Buzón de correo)
- Windows Small Business Server 2008
- Windows Small Business Server 2011


i NOTA

si ejecuta Microsoft Exchange Server 2007 o 2010 puede elegir entre la Protección de la base de datos de correo electrónico y la Exploración de la base de datos a petición. No obstante, solo uno de estos dos tipos de protección puede estar activo a la vez. Si decide utilizar la Exploración de la base de datos a petición, deberá deshabilitar la integración de la Protección de la base de datos de correo electrónico en la Configuración avanzada del [Servidor](#). De lo contrario, la Exploración de la base de datos a petición no estará disponible.

Dirección del host: nombre o dirección IP del servidor que ejecuta EWS (Exchange Web Services).

Nombre de usuario: especifica las credenciales de un usuario que tenga acceso adecuado a EWS (Servicios web de Exchange).


Contraseña del usuario: haga clic en **Configurar** junto a la **Contraseña del usuario** e ingrese la contraseña para esta cuenta del usuario.

 **IMPORTANTE**

Para explorar carpetas públicas, la cuenta del usuario que se usa para explorar la base de datos a petición debe tener un buzón de correo. De lo contrario, verá el mensaje de error *Failed to load public folders* en el [registro de exploración de base de datos](#), junto con un mensaje más específico devuelto por Exchange.

Asignar papel de aplicación/personificación al usuario: si esta opción está marcada en gris, debe especificar el **nombre de usuario** primero. Haga clic en **Asignar** para asignar automáticamente el papel de aplicación/personificación al usuario seleccionado. Como alternativa, puede asignar manualmente el papel de aplicación/personificación a una cuenta de usuario. Para obtener más información, consulte [Detalles de la cuenta de la exploración de la base de datos](#).

Usar SSL: debe estar habilitado si EWS (Servicios web de Exchange) está configurado para **Solicitar SSL** en IIS. Si el SSL está habilitado, se debe importar el certificado de Exchange Server al sistema con ESET Mail Security (en caso de que los roles de Exchange Server estén en servidores diferentes). Las configuraciones para EWS pueden encontrarse en IIS en *Sitios/Sitio web predeterminado/EWS/Configuraciones de SSL*.

 **NOTA**

deshabilite **Usar SSL** solo en caso de que tenga EWS configurado en IIS para no Solicitar SSL.

Certificado del cliente: debe configurarse solo cuando los Servicios web de Exchange exijan el certificado del cliente. **Seleccionar** le permite seleccionar cualquiera de los certificados.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CONFIGURACIÓN DE EXPLORACIÓN DE LA BASE DE DATOS A PETICIÓN

Dirección del host

WIN-JDLB8CEUR5

Nombre de usuario

Contraseña de usuario

Establecer

Asignar papel de aplicación/personificación al usuario

Asignar

Utilizar SSL

☒

Ignorar los errores del certificado del servidor

☐

X

Certificado del cliente

Seleccionar

Acción para emprender si no es posible la desinfección

Eliminar objeto

Cantidad de subprocessos de exploración

ELEMENTOS ADICIONALES DEL BUZÓN DE CORREO

SERVIDOR PROXY

Sin acción

Mover el mensaje a la papelera

Eliminar mensaje

Eliminar objeto

Reemplazar objeto con información sobre la acción

Predeterminado

Aceptar

Cancelar

Acción para realizar cuando no es posible desinfectar: este campo de acción le permite **bloquear** el contenido infectado.

Sin acción: no realizar ninguna acción con el contenido infectado del mensaje.

Mover el mensaje a la papelera: no se admite para los elementos de la carpeta Pública; en cambio, se aplicará la acción **Eliminar objeto**.

Eliminar objeto: elimina el contenido infectado del mensaje.

Eliminar el mensaje: eliminar el mensaje completo, incluyendo su contenido infectado.

Reemplazar objeto con información de acción: elimina un objeto e incluye la información acerca de la eliminación de este objeto.

4.1.8.1 Elementos adicionales del buzón de correo

Las configuraciones del explorador de la base de datos a petición le permiten habilitar o deshabilitar la exploración de otros tipos de elementos de la casilla de correo:

- Explorar calendario
- Explorar tareas
- Explorar contactos
- Explorar diario

NOTA

Si tiene problemas de rendimiento, puede deshabilitar la exploración de estos elementos. Las exploraciones tardarán más tiempo cuando estos elementos estén habilitados.

4.1.8.2 Servidor proxy

En caso de que utilice un servidor proxy entre Exchange Server con rol CAS y el Exchange Server donde está instalado ESET Mail Security, especifique los parámetros del servidor proxy. Esto es necesario porque ESET Mail Security se conecta con el API de EWS (Servicios web de Exchange) mediante HTTP/HTTPS. De lo contrario, la Exploración de la base de datos a petición no funcionará.

Servidor proxy: ingrese la dirección IP o el nombre del servidor proxy que utilice.

Puerto: ingrese el número de puerto del servidor proxy.

Nombre de usuario, Contraseña: ingrese las credenciales si su servidor proxy requiere autenticación.

4.1.8.3 Detalles de la cuenta de la exploración de la base de datos

Esta ventana de diálogo muestra si no ha especificado un nombre de usuario y una contraseña específicos para la **Exploración de la base de datos** en la **Configuración avanzada**. Especifique las credenciales del usuario que tiene acceso a EWS (Servicios web de Exchange) en esta ventana emergente y haga clic en **Aceptar**. De manera alternativa, vaya a **Configuración avanzada** al presionar **F5** y navegar a **Servidor > Exploración de la base de datos a petición**. Ingrese el **Nombre de usuario**, haga clic en **Configurar**, ingrese la contraseña para esta cuenta de usuario y haga clic en **Aceptar**.

- Puede seleccionar **Guardar la información de la cuenta** para guardar la configuración de la cuenta, para que no tenga que ingresar la información de la cuenta cada vez que ejecute una exploración de la base de datos a petición.
- Si una cuenta de usuario no tiene el acceso adecuado a EWS, puede seleccionar **Crear asignación de rol "Suplantación de aplicación"** para asignar este rol a una cuenta. Como alternativa, puede asignar manualmente el rol de Suplantación de aplicación, consulte la nota a continuación para obtener más detalles.

Scan account details

?

User name

FRANTO\administrator

Password

☐ Save account information

☐ Create "ApplicationImpersonation" role assignment

OK

Cancel

! IMPORTANTE

La cuenta de exploración debe tener el rol **Suplantación de aplicación** asignado para que el motor de exploración explore los buzones de correo de los usuarios dentro de las bases de datos de buzones de correo de Exchange. Si se ejecuta Exchange Server 2010 o superior, se crea una nueva Directiva de límites EWS sin límites para la cuenta de usuario. Asegúrese de configurar la Directiva de límite EWS para la cuenta de exploración y evitar varias solicitudes de operación de ESET Mail Security, que de otra manera podrían causar la expiración de las solicitudes. Consulte los artículos [Procedimientos recomendados de EWS](#) y [Comprensión de las directivas de límite de cliente](#) para obtener más información acerca de las Directivas de límite. Además, consulte el artículo [Cambiar la configuración de límite de usuario para usuarios específicos](#) para obtener más detalles y ejemplos.

i NOTA

Si desea asignar manualmente el rol de Suplantación de aplicación a una cuenta de usuario y crear una nueva Directiva de límite EWS para esta cuenta, puede usar los siguientes comandos (reemplazar `ESET-user` con un nombre de cuenta real en el sistema, también puede ajustar los límites para la directiva de límite EWS mediante el reemplazo de `$null` con números):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation
Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:ESET-user
```

Esto puede demorar unos minutos en aplicarse.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -EWSFastSearchTimeoutInSeconds
```

```
Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2013

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation  
-User:ESET-user
```

Esto puede demorar unos minutos en aplicarse.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlim
```

```
Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-ThrottlingPolicy
```

4.1.9 Cuarentena de correo

El administrador de Cuarentena de correo electrónico está disponible para los tres tipos de cuarentena:

- [Cuarentena local](#)
- [Correo electrónico de cuarentena](#)
- [Cuarentena de MS Exchange](#)

Puede ver el contenido de la Cuarentena de correo electrónico en el [Administrador de cuarentena de correo electrónico](#) para todos los tipos de cuarentena. Además, la cuarentena local también puede verse en la [Interfaz web de cuarentena de correo electrónico](#).

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam 1

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CUARENTENA DE CORREO

Tipo de cuarentena

Almacenar mensajes de receptores inexistentes

Saltear la evaluación de reglas cuando se liberan correos electrónicos

ALMACENAMIENTO DE ARCHIVOS

INTERFAZ WEB

Cuarentena local

Cuarentena local

Correo electrónico de cuarentena

Cuarentena de MS Exchange

☒

Predeterminado

Aceptar

Cancelar

Almacenar mensajes de destinatarios inexistentes: cuando está habilitada, los mensajes que se enviaron a los destinatarios que no existen en el Active Directory se almacenan en el correo en cuarentena. Deshabilite esta característica si no desea conservar estos mensajes en el correo en cuarentena. Cuando está deshabilitada, los mensajes para un destinatario desconocido se eliminarán silenciosamente.

Omitir evaluación de reglas al liberar el correo: si desea liberar un mensaje de la cuarentena, las reglas no evaluarán este mensaje. Es para evitar que el mensaje vuelva a la cuarentena y el mensaje liberado se entregue al destinatario de manera exitosa. Esta característica se usa solamente cuando el Administrador libera el mensaje. Si deshabilita esta característica o si un usuario que no es el Administrador libera un mensaje, las reglas evaluarán el mensaje.

i NOTA

Las dos configuraciones están disponibles para Microsoft Exchange Server 2007 y versiones posteriores.

4.1.9.1 Cuarentena local

La cuarentena local utiliza el sistema de archivos local para almacenar los correos electrónicos en cuarentena y una base de datos de SQLite como índice. Los archivos de correo electrónico en cuarentena almacenados como también el archivo de la base de datos se cifran por motivos de seguridad. Estos archivos se ubican en `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (en Windows Server 2008 y 2012) o `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (en Windows Server 2003).

i NOTA

Si desea almacenar los archivos en cuarentena en un disco diferente, que no sea la unidad predeterminada `c:`, debe cambiar la **Carpeta de datos** con su ruta preferida durante la [instalación](#) de ESET Mail Security.

Características de la cuarentena local:

- Los mensajes de SPAM y de correo electrónico en cuarentena se almacenarán en un sistema de archivos local, lo que significa que estos no se contendrán en la base de datos del buzón de correo de Exchange.
- Cifrado y compresión de archivos de correo electrónico en cuarentena almacenados localmente.
- [Interfaz web de cuarentena de correo](#): una alternativa al [administrador de cuarentena de correo](#).
- Los informes de cuarentena pueden enviarse a una dirección de correo electrónico especificada utilizando una [tarea programada](#).
- Los archivos de correo electrónico en cuarentena eliminados de la ventana de cuarentena (después de los 21 días en forma predeterminada), aún se almacenan en un sistema de archivos (hasta que ocurre la eliminación automática después de una cantidad de días especificada).
- Eliminación automática de archivos de correo electrónico antiguos (después de 3 días en forma predeterminada). Para obtener más información, consulte la configuración del [Almacenamiento de archivos](#).
- Puede restablecer los archivos de correo electrónico en cuarentena eliminados mediante [eShell](#) (siempre que no hayan sido eliminados aún del sistema de archivos).

i NOTA

La desventaja de utilizar una cuarentena local es que si ejecuta servidores múltiples de ESET Mail Security con el rol del servidor Transporte Hub, debe administrar la cuarentena local de cada servidor de manera separada. Cuantos más servidores, más cuarentenas para administrar.

Puede inspeccionar los mensajes de correo electrónico en cuarentena y decidir **eliminar** o **liberar** cualquiera de ellos. Para ver y administrar localmente los mensajes de correo electrónico en cuarentena, puede utilizar el [Administrador de cuarentena de correo](#) desde la interfaz gráfica del usuario principal o la [interfaz web de la cuarentena de correo](#).

4.1.9.1.1 Almacenamiento de archivos

En esta sección puede modificar la configuración del almacenamiento de archivos que utiliza la cuarentena local.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo1

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CUARENTENA DE CORREO

Tipo de cuarentenaCuarentena local

ALMACENAMIENTO DE ARCHIVOS

Comprimir los archivos en cuarentena☒

Eliminar archivos antiguos tras (3 días)21

Eliminar archivos eliminados tras (en días)3

Almacenar mensajes de receptores inexistentes☒

INTERFAZ WEB

Predeterminado

Aceptar

Cancelar

Comprimir los archivos en cuarentena: los archivos en cuarentena comprimidos ocupan menos espacio en disco, pero si decide no comprimir los archivos, utilice el interruptor para deshabilitar la compresión.

Eliminar archivos antiguos tras (en días): cuando los mensajes alcanzan una cantidad específica de días, son eliminados de la ventana de cuarentena. No obstante, los archivos no se eliminarán del disco durante la cantidad de días especificada en **Eliminar archivos borrados tras (días)**. Como los archivos no son eliminados del sistema de archivos, es posible recuperar esos archivos mediante [eShell](#).

Eliminar archivos borrados tras (en días): elimina los archivos del disco después de la cantidad de días especificada, no es posible realizar ninguna tarea de recuperación después de que estos archivos sean eliminados (a menos que tenga una solución de copia de respaldo del sistema de archivos en funcionamiento).

Almacenar mensajes para destinatarios no existentes: por lo general, los mensajes de spam se envían a destinatarios aleatorios de un dominio determinado en un intento por acertar con uno existente. Los mensajes enviados a los usuarios que no existen en un Directorio activo se almacenan en la Cuarentena local en forma predeterminada. No obstante, puede deshabilitar esta función para que los mensajes enviados a destinatarios no existentes no se almacenen, de esta manera, su cuarentena local no estará rebasada por muchos mensajes de spam de este tipo. Esto también ahorra espacio en disco.

4.1.9.1.2 Interfaz Web

La interfaz web de cuarentena de correo es una alternativa al [Administrador de cuarentena de correo](#), no obstante, solo está disponible para la [Cuarentena local](#).

NOTA

La interfaz Web de la cuarentena no está disponible en un servidor con rol de servidor Transporte perimetral. Esto se debe a que Active Directory no es accesible para su autenticación.

La interfaz web de cuarentena de correo le permite ver el estado de la cuarentena de correo. También le permite administrar los objetos de correo electrónico en cuarentena. Se puede acceder a esta interfaz web mediante enlaces de los informes de cuarentena o directamente al ingresar una URL en el navegador web. Para acceder a la interfaz web de la cuarentena de correo, debe autenticarse mediante credenciales de dominio. Internet Explorer autenticará automáticamente un usuario de dominio. Sin embargo, el certificado de la página web debe ser válido, el [Inicio de sesión automático](#) debe estar habilitado en IE y debe agregar el sitio web de Cuarentena a los sitios de Intranet local.

Cualquier usuario que exista en el Active Directory puede tener acceso a la interfaz web de Cuarentena de correo pero solamente verá los elementos en cuarentena que se enviaron a su dirección de correo (esto incluye también el alias del usuario). El Administrador está habilitado para ver todos los elementos en cuarentena de todos los destinatarios.

El interruptor **Habilitar interfaz web** le permite deshabilitar o habilitar la interfaz web.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antisпам

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

Almacenar mensajes de receptores inexistentes

Saltear la evaluación de reglas cuando se liberan correos electrónicos

ALMACENAMIENTO DE ARCHIVOS

Comprimir los archivos en cuarentena

Eliminar archivos antiguos tras (3 días)

Eliminar archivos eliminados tras (en días)

INTERFAZ WEB

Activar la interfaz Web

Url Web

Puerto HTTPS

Puerto HTTP

Habilitar administradores predeterminados

Derechos de acceso adicionales

Predeterminado

Aceptar

Cancelar

URL web: esta es la URL en la que la interfaz web de la cuarentena de correo estará disponible. De manera predeterminada, es FQDN del servidor con /quarantine (por ejemplo, mailserver.company.com/quarantine). Puede especificar su propio directorio virtual en lugar del /quarantine predeterminado. Puede cambiar la **url de la Web** en cualquier momento al editar el valor. Se debe especificar el valor de la **url de la Web** sin un esquema (HTTP, HTTPS) y sin un número de puerto, use solo la forma fqdn/virtualdirectory. También puede usar comodines en lugar de FQDN.


NOTA

ESET Mail Security es compatible con url de la Web en cuatro formas diferentes:

- Comodín fuerte (+/quarantine)
- Explícito (mydomain.com/quarantine)
- Comodín débil vinculado con IP (192.168.0.0/quarantine)
- Comodín débil (* /quarantine)

Para más información, consulte la sección **Categorías especificadoras del host** del artículo [Cadenas de UrlPrefix](#).

NOTA

Después de modificar la **url de la Web**, no es posible volver al valor predeterminado al hacer clic en el ícono [revertir](#) . Quite la entrada y deje el cuadro de texto en blanco. Reinicie el servidor. Cuando se inicia ESET Mail Security y detecta que la url de la Web está vacía, completará automáticamente este campo con el valor predeterminado fqdn/quarantine.


Puerto HTTPS: se usa para la interfaz Web. El número de puerto predeterminado es 443.


Puerto HTTP: se usa para liberar correos de cuarentena mediante informes de correos.

IMPORTANTE

Si cambia el número de puerto a HTTPS o HTTP, asegúrese de agregar el correspondiente [enlace al puerto en IIS](#).

- **Habilitar los administradores predeterminados:** de manera predeterminada, los miembros del grupo de Administradores tienen acceso de administrador a la interfaz web de la Cuarentena de correo. El acceso de administrador no tiene restricciones y le permite al Administrador ver todos los elementos en cuarentena de todos los destinatarios. Si deshabilita esta opción, solamente la cuenta del usuario de Administrador tendrá acceso de administrador a la interfaz web de la Cuarentena de correo.
- **Derechos de acceso adicionales:** puede conceder acceso adicional a los usuarios a la interfaz web de Cuarentena de correo y elegir el tipo de acceso. Haga clic en **Editar** para abrir la ventana de **Derechos de acceso adicionales**, haga clic en botón **Agregar** para conceder acceso a un usuario. En la ventana emergente **Nuevo derecho de acceso**, haga clic en **Seleccionar** y elija un usuario de Active Directory (solamente puede elegir un usuario) y seleccione el **Tipo de acceso** de la lista desplegable:
 - **Administrador:** el usuario tendrá acceso de administrador a la Interfaz web de cuarentena de correo.
 - **Acceso delegado:** use este tipo de acceso si desea que un usuario (delegado) vea y administre los mensajes en cuarentena de otro destinatario. Especifique la **Dirección del destinatario** ingresando la dirección de correo electrónico para un usuario, cuyos mensajes en cuarentena los administrará un delegado. Si un usuario tiene un alias en el Active Directory, puede agregar derechos de acceso adicionales para cada alias si lo desea.

New access right

Nombre de usuario

Seleccionar

Tipo de acceso

Administrador

Administrador

Acceso delegado

Aceptar

Cancelar

Un ejemplo de usuarios a los que se les concedieron derechos de acceso adicionales a la interfaz web de la Cuarentena de correo:

Nombre de usuario	Tipo de acceso	Dirección del destinatario
FRANTO\administrator	Administrador	

Agregar Quitar

Aceptar Cancelar

Para acceder a la interfaz Web de cuarentena de correo, abra el navegador Web y utilice la URL especificada en **Configuración avanzada > Servidor > Cuarentena de correo > Interfaz Web > URL Web**.

ESET MAIL QUARANTINE ADMINKO SWITCH ACCOUNTS LOGOUT

SEARCH in SUBJECT

DATE RECEIVED	SUBJECT	SENDER	RECIPIENTS	TYPE	REASON	RELEASE SELECT ALL	DELETE SELECT ALL	NO ACTION SELECT ALL
2015-06-05 01:12	viagra	xp64i@sx.local	vista3@s4.local	rule	rule 01	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2015-06-05 01:12	virus	xp64i@sx.local	vista3@s4.local	virus	Eicar	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2015-06-05 01:12	test	xp64i@sx.local	vista3@s4.local	spam	Found	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

PAGE SIZE 10

Liberar: libera los correos electrónicos a sus destinatarios originales mediante el directorio de reproducción nueva y los elimina de la cuarentena. Haga clic en **Enviar** para confirmar la acción.

NOTA

Cuando se libera un correo de cuarentena, ESET Mail Security ignora el encabezado **TO:** MIME porque se puede alterar fácilmente. En cambio, usa la información del destinatario original del comando **RCPT TO:** adquirida durante la conexión de SMTP. De esta manera, se garantiza que el destinatario correcto del correo reciba el mensaje liberado de cuarentena.

Eliminar: elimina el elemento de la cuarentena. Haga clic en **Enviar** para confirmar la acción.

Cuando haga clic en **Asunto**, se abrirá una ventana emergente con detalles acerca de los correos electrónicos en cuarentena, como el **Tipo**, el **Motivo**, el **Emisor**, la **Fecha**, los **Adjuntos**, etc.

Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28

ATTACHMENTS

[Show headers](#)

RELEASE

DELETE

[Go to quarantine view.](#)

Haga clic en **Mostrar encabezados** para revisar el encabezado del correo electrónico de cuarentena.

Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

Received: from win2k3r2x64-ss4 ([10.1.117.232]) by win2k3sp2x86ss1.s2.local with Microsoft SMTPSVC(6.0.3790.4675);
Mon, 22 Jun 2015 23:28:46 -0700

Received:
To: <vista@s2.local>
Subject:[SPAM] hlavicka
X-Originating-IP:
MIME-Version: 1.0
Content-Type: text/plain
Message-ID: <-974233353.8808@win2k8x64-EDGE.s1.local>
From:
Return-Path: <>
Date: Tue, 9 Nov 2010 22:12:48 -0800
X-MS-Exchange-Organization-OriginalArrivalTime: 10 Nov 2010 06:12:48.9975 (UTC)
X-MS-Exchange-Organization-AuthSource: win2k8x64-EDGE.s1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
Received-SPF: Fail (win2k8x64-EDGE.s1.local: domain of does not designate 10.1.117.225 as permitted sender) receiver=win2k8x64-EDGE.s1.local

RELEASE

DELETE

Go to quarantine view.

Si lo desea, haga clic en **Liberar** o **Eliminar** para realizar una acción sobre un mensaje de correo electrónico en cuarentena.

i

NOTA

debe cerrar la ventana del navegador para salir por completo de la interfaz web de cuarentena de correo. De lo contrario, haga clic en **Ir a vista de cuarentena** para regresar a la pantalla anterior.

You must close your browser to complete the sign out process.

Go to quarantine view.

!

IMPORTANTE

si tiene problemas para acceder a la interfaz web de cuarentena de correo desde su navegador o recibe el error HTTP Error 403.4 - Prohibido o similar, controle para ver qué **Tipo de cuarentena** tiene seleccionado y asegurarse de que sea una **Cuarentena local** y que la opción **Habilitar interfaz web** esté habilitada.

4.1.9.2 Buzón de correo de cuarentena y cuarentena de MS Exchange

Si decide no utilizar la [cuarentena local](#) tiene dos opciones, la **Cuarentena de casilla de correo** o la **Cuarentena de MS Exchange**. Cualquiera que sea la opción que elija, deberá crear un usuario dedicado con casilla de correo (por ejemplo [main_quarantine@company.com](#)) la cual luego se utilizará para almacenar mensajes de correo electrónico en cuarentena. Este usuario y esta casilla de correo además serán utilizados por el [Administrador de la cuarentena de correo](#) para ver y administrar los elementos de la cuarentena. Deberá especificar los detalles de cuenta de este usuario en la [Configuración del administrador de cuarentena](#).

IMPORTANTE

no recomendamos que utilice la cuenta de usuario de Administrador como casilla de correo de cuarentena.

NOTA

la **Cuarentena de MS Exchange** no está disponible para Microsoft Exchange 2003, solamente la **Cuarentena local** y el **Buzón de correo de cuarentena**.

- Cuando selecciona la **Cuarentena de MS Exchange**, ESET Mail Security utilizará el **Sistema de cuarentena de Microsoft Exchange** (esto se aplica a Microsoft Exchange Server 2007 y posterior). En este caso, el mecanismo interno de Exchange se usa para almacenar mensajes potencialmente infectados y SPAM.

NOTA

en forma predeterminada, la cuarentena interna de Exchange no está activada. Para activarla, es necesario abrir la Consola de administración de Exchange y escribir el siguiente comando (reemplazar `name@domain.com` con una dirección real de su casilla de correo dedicada):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

- Cuando seleccione la **Cuarentena de casilla de correo**, deberá especificar el mensaje de la dirección de cuarentena (por ejemplo [main_quarantine@company.com](#)).

NOTA

La ventaja del buzón de correo en cuarentena/Cuarentena de MS Exchange con respecto a la [cuarentena local](#) es que los objetos en cuarentena de correo se administran en un lugar sin importar la cantidad de servidores con rol de servidor de Transporte Hub. Sin embargo, hay una desventaja del buzón de correo en cuarentena/Cuarentena de MS Exchange, los mensajes de SPAM y de correo electrónico en cuarentena se almacenan en la base de datos del buzón de correo de Exchange y solo el administrador puede administrar la cuarentena de correo.

4.1.9.2.1 Configuración de la administración de cuarentena

Dirección del host: aparecerá de manera automática si su Exchange Server con rol de CAS está localmente presente. De manera alternativa, si el rol de CAS no está presente en el mismo servidor con ESET Mail Security instalado pero puede encontrarse dentro de AD, la dirección del host aparecerá de manera automática. Si no aparece, puede ingresar el nombre del host de manera manual. La detección automática no funcionará con el rol del servidor Transporte Edge.

NOTA

dirección IP no admitida, debe utilizar el nombre de host del servidor CAS.

Nombre de usuario: [cuenta de usuario de cuarentena](#) dedicada que creó para almacenar los mensajes en cuarentena (o una cuenta que tiene acceso a esta casilla de correo mediante la delegación de acceso). En el rol del servidor Transporte Edge que no forma parte del dominio, resulta necesario utilizar toda la dirección de correo electrónico (por ejemplo [main_quarantine@company.com](#)).

Contraseña: ingrese la contraseña de su cuenta de cuarentena.

Usar SSL: debe estar habilitado si EWS (Servicios web de Exchange) está configurado para **Solicitar SSL** en IIS. Si el SSL está habilitado, se debe importar el certificado de Exchange Server al sistema con ESET Mail Security (en caso de que los roles de Exchange Server estén en servidores diferentes). Las configuraciones para EWS se pueden encontrar en IIS en *Sites/Default web site/EWS/SSL Settings*.

NOTA

deshabilite **Usar SSL** solo en caso de que tenga EWS configurado en IIS para no Solicitar SSL.

Ignorar errores de certificados del servidor: ignora los siguientes estados: firma propia, nombre equivocado en el certificado, uso incorrecto, vencido.

Configuración avanzada

SERVIDOR

Antivirus y antispyware

Protección antispam

Reglas

Protección del transporte de correo electrónico

Exploración de la base de datos a petición

Cuarentena de correo 2

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

CUARENTENA DE CORREO

Tipo de cuarentena

Correo electrónico de cuarentena

CONFIGURACIÓN DE LA ADMINISTRACIÓN DE CUARENTENA

Dirección del host

Nombre de usuario

Contraseña

Utilizar SSL

Ignorar los errores del certificado del servidor

SERVIDOR PROXY

Correo electrónico de cua...

name@email.com

EX1

mailquarantine

.....

☒

☐

☐

Predeterminado

Aceptar

Cancelar

4.1.9.2.2 Servidor proxy

En caso de que utilice un servidor proxy entre Exchange Server con rol CAS y el Exchange Server donde está instalado ESET Mail Security, especifique los parámetros del servidor proxy. Esto es necesario porque ESET Mail Security se conecta con el API de EWS (Servicios web de Exchange) mediante HTTP/HTTPS. De lo contrario, la casilla de correo de cuarentena y la cuarentena de MS Exchange no funcionarán.

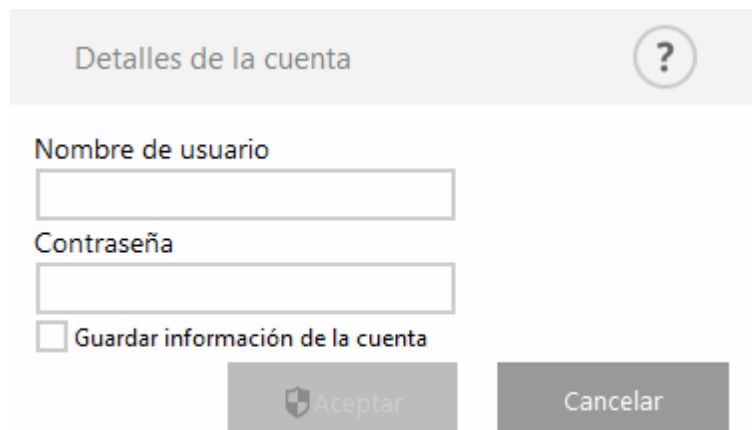
Servidor proxy: ingrese la dirección IP o el nombre del servidor proxy que utilice.

Puerto: ingrese el número de puerto del servidor proxy.

Nombre de usuario, Contraseña: ingrese las credenciales si su servidor proxy requiere autenticación.

4.1.9.3 Detalles de la cuenta del administrador de la cuarentena

Esta ventana de diálogo se mostrará si no configura una cuenta para sus **Detalles del administrador de cuarentena**. Especifique las credenciales para un usuario con acceso a la **Casilla de correo de cuarentena** y haga clic en **Aceptar**. De manera alternativa, presione F5 para acceder a la **Configuración avanzada** y navegar al **Servidor > Cuarentena de correo > Configuraciones del administrador de cuarentena**. Ingrese el **Nombre de usuario** y la **Contraseña** para su casilla de correo de cuarentena.



Puede seleccionar **Guardar información de la cuenta** para guardar las configuraciones de la cuenta para uso futuro cuando acceda al administrador de cuarentena.

4.2 Equipo

El módulo **Equipo** se puede encontrar bajo **Configuración > Equipo**. Muestra una vista general de los módulos de protección que se describen en el [capítulo anterior](#). En esta sección, las siguientes configuraciones están disponibles:

- [Exploración del equipo a petición](#)
- [Exploración en estado inactivo](#)
- [Exploración en el inicio](#)
- [Medios extraíbles](#)
- [Protección de documentos](#)
- [HIPS](#)

Las **opciones de exploración** para todos los módulos de protección (por ejemplo, la protección del sistema de archivos en tiempo real o la protección del acceso a la web, etc.) le permiten habilitar o deshabilitar la detección de lo siguiente:

- Las **aplicaciones potencialmente no deseadas (PUA)** no tienen necesariamente la intención de ser malintencionadas, pero pueden afectar el rendimiento de su equipo en forma negativa. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).
- **Aplicación potencialmente no segura**: hace referencia al software comercial y legítimo que se puede usar inadecuadamente para fines malintencionados. Algunos ejemplos de las aplicaciones potencialmente inseguras son las herramientas de acceso remoto, las aplicaciones para adivinar contraseñas y los registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). Esta opción se encuentra deshabilitada en forma predeterminada. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).
- **Aplicaciones potencialmente sospechosas**: incluyen programas comprimidos con [empaquetadores](#) o protectores. Estos tipos de protectores, por lo general, son vulnerados por los autores de malware para evadir la detección.

La **tecnología Anti-Stealth** es un sistema sofisticado que detecta programas peligrosos como los [rootkits](#), que tienen la capacidad de ocultarse del sistema operativo, haciendo que sea imposible detectarlos mediante técnicas de evaluación comunes.

Las **exclusiones de procesos** le permiten excluir procesos específicos. Por ejemplo, los procesos de la solución de

copias de respaldo, en los que todas las operaciones de archivos atribuidas a dichos procesos excluidos se ignorarán y se considerarán seguras, minimizando de esta manera la interferencia con los procesos de copia de respaldo.

Las **Exclusiones** permiten excluir archivos y carpetas de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear las exclusiones cuando sea absolutamente necesario. Las situaciones donde sea posible que necesite excluir un objeto incluirían la exploración de las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una exploración, o un software que entra en conflicto con la exploración. Para obtener instrucciones para excluir un objeto de la exploración, consulte las [Exclusiones](#).

4.2.1 Detección de una infiltración

Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Conducta estándar

Como ejemplo general de la forma en que ESET Mail Security maneja las infiltraciones, estas se pueden detectar mediante:

- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Exploración del equipo a petición

Cada uno usa el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a [Cuarentena](#) o finalizar la conexión. Una ventana de notificación se muestra en el área de notificaciones en la esquina inferior derecha de la pantalla. Para obtener más información sobre los niveles de desinfección y conducta, consulte [Desinfección](#).

Desinfección y eliminación

Si no hay ninguna acción predefinida para la protección del sistema de archivos en tiempo real, el programa le pedirá que seleccione una opción en una ventana de alerta. Por lo general están disponibles las opciones **No infectados**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que esto dejará los archivos infectados sin desinfectar. La excepción a este consejo es cuando usted está seguro de que un archivo es inofensivo y fue detectado por error.

Aplique la opción de desinfección si un virus atacó un archivo y le adjuntó códigos maliciosos. En este caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo está compuesto exclusivamente por códigos maliciosos, será eliminado.

Si un archivo infectado está “bloqueado” u otro proceso del sistema lo está usando, por lo general se elimina cuando es liberado (normalmente luego del reinicio del sistema).

Varias amenazas

Si algún archivo infectado no se desinfectó durante la exploración del equipo (o el [Nivel de desinfección](#) estaba configurado en **Sin desinfección**), se muestra una ventana de alerta que le solicitará seleccionar las acciones para dichos archivos. Seleccione una acción individualmente para cada amenaza de la lista o puede usar **Seleccione una acción para todas las amenazas de la lista** y seleccionar una acción para aplicar a todas las amenazas de la lista, y después haga clic en **Finalizar**.

Eliminación de archivos en archivos comprimidos

En el modo de desinfección predeterminado, se eliminará el archivo comprimido completo solo si todos los archivos que lo componen están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos inofensivos no infectados. Tenga precaución al realizar una exploración con Desinfección estricta: si la Desinfección estricta está habilitada, un archivo se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

Si su equipo muestra signos de infección por malware, por ej., funciona más lento, con frecuencia no responde, etc., se recomienda hacer lo siguiente:

- abra ESET Mail Security y haga clic en Exploración del equipo
- Haga clic en **Exploración inteligente** (para obtener más información, consulte en [Exploración del equipo](#))
- Una vez finalizada la exploración, consulte el registro para verificar la cantidad de archivos explorados, infectados y desinfectados

Si solo quiere explorar una parte determinada del disco, haga clic en **Exploración personalizada** y seleccione los objetos para explorar en busca de virus.

4.2.2 Exclusiones de procesos

Esta característica le permite excluir procesos de aplicaciones de la exploración de acceso del antivirus. Estas exclusiones ayudan a minimizar el riesgo de conflictos potenciales y a mejorar el rendimiento de aplicaciones excluidas, lo que a su vez tiene un efecto positivo sobre el rendimiento general del sistema operativo.

Cuando se excluye un proceso, su archivo ejecutable no es monitoreado. La actividad de los procesos excluidos no es monitoreada por ESET Mail Security y no se realiza ninguna exploración sobre ninguna operación de archivo realizada por el proceso.

Use los botones **Agregar**, **Editar** y **Quitar** para administrar exclusiones de procesos.

i NOTA

las exclusiones de procesos son exclusiones de la exploración de acceso del antivirus únicamente. Por ejemplo, la protección del acceso a la web no toma en cuenta esta exclusión, entonces, si excluye el archivo ejecutable de su navegador web, los archivos descargados aún se explorarán. De esta manera, las infiltraciones podrán detectarse de todos modos. Esta situación representa solamente un ejemplo, y no recomendamos crear exclusiones para los navegadores web.

i NOTA

HIPS participa en la evaluación de los procesos excluidos, en consecuencia, le recomendamos probar los procesos excluidos recientemente con HIPS habilitado (o deshabilitado si tiene problemas). Deshabilitar HIPS no afectará las exclusiones de los procesos. Si HIPS está deshabilitado, la identificación de los procesos excluidos se basará únicamente en la ruta.

4.2.3 Exclusiones automáticas

Los desarrolladores de aplicaciones y sistemas operativos para servidores recomiendan excluir de la exploración antivirus grupos críticos de archivos operativos y carpetas para la mayoría de sus productos. Las exploraciones antivirus pueden tener un efecto negativo en el rendimiento de un servidor, generar conflictos e incluso impedir la ejecución de algunas aplicaciones en el servidor. Las exclusiones ayudan a minimizar el riesgo de conflictos potenciales e incrementar el rendimiento general del servidor mientras se ejecuta un programa antivirus.

ESET Mail Security identifica las aplicaciones críticas del servidor y los archivos críticos del sistema operativo, y los agrega automáticamente a la lista de [Exclusiones](#). Se puede ver una lista de varias aplicaciones detectadas bajo **Exclusiones automáticas para generar**, para las cuales se crearon las exclusiones. Todas las exclusiones automáticas están habilitadas de forma predeterminada. Puede habilitar o deshabilitar cada aplicación del servidor con un clic en el interruptor con el siguiente resultado:

1. Si la exclusión de una aplicación o un sistema operativo permanece habilitada, se agregará cualquiera de sus archivos o carpetas críticos a la lista de archivos excluidos de la exploración (**Configuración avanzada > Equipo > Básico > Exclusiones > Editar**). Cada vez que se reinicie el servidor, el sistema realizará una verificación automática de las exclusiones y restaurará todas las exclusiones que se hayan eliminado de la lista. Si quiere asegurarse de que se apliquen siempre las exclusiones automáticas recomendadas, ésta es la configuración más indicada.
2. Si el usuario deshabilita la exclusión de una aplicación o un sistema operativo, los archivos y carpetas críticos correspondientes permanecerán en la lista de archivos excluidos de la exploración (**Configuración avanzada > Equipo > Básico > Exclusiones > Editar**). No obstante, no se verificarán ni renovarán automáticamente en la lista de **Exclusiones** cada vez que se reinicie el equipo (ver el punto 1 arriba). Esta configuración es recomendable para los usuarios avanzados que deseen eliminar o modificar algunas de las exclusiones estándar. Si desea eliminar las exclusiones de la lista sin reiniciar el servidor, deberá hacerlo manualmente (**Configuración avanzada > Equipo > Básico > Exclusiones > Editar**).

Cualquier exclusión definida por el usuario que se ingrese manualmente (bajo **Configuración avanzada > Equipo > Básico > Exclusiones > Editar**) no resultará afectada por las configuraciones descritas anteriormente.

Las exclusiones automáticas de aplicaciones o sistemas operativos del servidor se seleccionan basándose en las recomendaciones de Microsoft. Para obtener más detalles, consulte los siguientes artículos de la base de conocimiento de Microsoft:

- [Recomendaciones para la detección de virus en equipos de empresa que ejecutan actualmente versiones compatibles de Windows](#)
- [Recomendaciones para solucionar problemas de un equipo con Exchange Server con software antivirus instalado](#)
- [Exploración Antivirus de nivel de archivo en Exchange 2007](#)
- [Software antivirus en el sistema operativo de servidores Exchange](#)

4.2.4 Caché local compartido

El caché local compartido aumentará el rendimiento en los entornos virtualizados mediante la eliminación de la exploración duplicada en la red. Esto garantiza que cada archivo se explorará solo una vez y se almacenará en el caché compartido. Active el interruptor **Habilitar caché local** para guardar la información en el caché local sobre las exploraciones de los archivos y las carpetas en su red. Si realiza una exploración nueva, ESET Mail Security buscará los archivos explorados en el caché. Si los archivos coinciden, se excluirán de la exploración.

La **configuración del Servidor** del caché contiene lo siguiente:

- **Nombre de host:** nombre o dirección IP del equipo donde se ubica el caché.
- **Puerto:** número del puerto usado para la comunicación (el mismo que fue configurado en el caché local compartido).
- **Contraseña:** especifica la contraseña del Caché local compartido si se lo requiere.

4.2.5 Rendimiento

Puede configurar una cantidad de motores de exploración ThreatSense independientes usados por la protección antivirus y antispyware en un momento.

Si no existen otras restricciones, recomendamos aumentar la cantidad de motores de exploración ThreatSense según esta fórmula: *cantidad de motores de exploración ThreatSense = (cantidad de CPU físicas x 2) + 1*.

NOTA

un valor aceptable es 1-20, por lo cual, la cantidad máxima de motores de exploración ThreatSense que puede usar es de 20.

4.2.6 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos del sistema relacionados con el antivirus. Se exploran todos los archivos en busca de códigos maliciosos cuando se abren, se crean o se ejecutan en el equipo. La protección del sistema de archivos en tiempo real se activa junto con el inicio del sistema.

The screenshot shows the 'Configuración avanzada' (Advanced Settings) window for Windows Security. The left sidebar lists various settings categories: SERVIDOR, EQUIPO, Protección del sistema de archivos en tiempo real (selected), Exploración del equipo a pedido, Exploración en estado inactivo, Exploración en el inicio, Medios extraíbles, Protección de documentos, HIPS, ACTUALIZACIÓN, INTERNET Y CORREO ELECTRÓNICO, CONTROL DEL DISPOSITIVO, and HERRAMIENTAS. The main pane is titled 'BÁSICO' and contains the following settings:

- Iniciar automáticamente la protección del sistema de archivos en tiempo real:** A toggle switch is turned on (blue).
- MEDIOS PARA EXPLORAR:**
 - Unidades locales:** A toggle switch is turned on (blue).
 - Medios extraíbles:** A toggle switch is turned on (blue).
 - Unidades de red:** A toggle switch is turned on (blue).
- EXPLORAR AL:**
 - Abrir el archivo:** A toggle switch is turned on (blue).
 - Crear el archivo:** A toggle switch is turned on (blue).
 - Ejecutar el archivo:** A toggle switch is turned on (blue).
 - Acceder a medios extraíbles:** A toggle switch is turned on (blue).
 - Apagar el equipo:** A toggle switch is turned on (blue).

At the bottom of the window, there are three buttons: 'Predeterminado' (Default), 'Aceptar' (Accept), and 'Cancelar' (Cancel).

En forma predeterminada, la protección del sistema de archivos en tiempo real se activa junto con el inicio del sistema y proporciona una exploración ininterrumpida. En casos especiales (por ejemplo, si existe un conflicto con otro explorador en tiempo real), se puede deshabilitar la protección en tiempo real quitando **Iniciar automáticamente la protección del sistema de archivos en tiempo real** en la configuración avanzada de **Protección del sistema de archivos en tiempo real > Básico**.

• Medios para explorar

En forma predeterminada, todos los tipos de medios se exploran en busca de amenazas potenciales:

Unidades locales: controla todos los discos rígidos del sistema.

Medios extraíbles: controla los CD/DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.

Unidades de red: explora todas las unidades asignadas.

Recomendamos que use la configuración predeterminada y solo modificarla en los casos específicos, por ejemplo, si al explorar ciertos medios, se ralentizan significativamente las transferencias de archivos.

- **Explorar al**

En forma predeterminada, se exploran todos los archivos cuando se abren, se crean o se ejecutan. Se recomienda mantener estas configuraciones predeterminadas, ya que proveen el máximo nivel de protección en tiempo real del equipo:

- **Abrir el archivo:** habilita o deshabilita la exploración cuando se abren los archivos.
- **Crear el archivo:** habilita o deshabilita la exploración cuando se crean los archivos.
- **Ejecutar el archivo:** habilita o deshabilita la exploración cuando se ejecutan los archivos.
- **Acceso de medios extraíbles:** habilita o deshabilita la exploración activada al acceder a medios extraíbles particulares con espacio de almacenamiento.
- **Apagar el equipo:** habilita o deshabilita la exploración accionada por el apagado del equipo.

La protección del sistema de archivos en tiempo real verifica todos los tipos de medios y el control se acciona por diversos sucesos, como el acceso a un archivo. Al usar los métodos de detección de la tecnología ThreatSense (como se describe en la sección [ThreatSense parámetros](#)), puede configurarse la protección del sistema de archivos en tiempo real para tratar nuevos archivos creados de modo diferente a los ya existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para controlar más de cerca a los nuevos archivos creados.

Para asegurar el mínimo impacto en el sistema al usar la protección en tiempo real, los archivos que ya se exploraron no se vuelven a explorar reiteradamente (a menos que se hayan modificado). Los archivos se vuelven a explorar de inmediato luego de cada actualización de la base de datos de firmas de virus. Este comportamiento se controla mediante el uso de la **Optimización inteligente**. Si se deshabilita la Optimización inteligente, se exploran todos los archivos cada vez que se accede a ellos. Para modificar esta configuración, presione **F5** para abrir configuración Avanzada y expanda **Equipo > Protección del sistema de archivos en tiempo real**. Haga clic en **ThreatSense parámetros de > Otros** y seleccione o anule la selección de **Habilitar la optimización inteligente**.

4.2.6.1 Exclusiones

No debe confundirse con **Extensiones excluidas**

Las exclusiones le permiten excluir archivos y carpetas de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear las exclusiones cuando sea absolutamente necesario. Las situaciones donde es posible que necesite excluir un objeto pueden incluir la exploración de las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una exploración o software que entra en conflicto con la exploración (por ejemplo, un programa de creación de copias de seguridad).

Para excluir un objeto de la exploración:

Haga clic en **Agregar** e ingrese la ruta a un objeto o selecciónelo en la estructura con forma de árbol. Puede usar caracteres globales para abarcar un grupo de archivos. Un signo de interrogación (?) representa un carácter único variable, mientras que un asterisco (*) representa una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos en una carpeta, escriba la ruta a la carpeta y use la máscara **"*. *"**.
- Para excluir un disco completo incluyendo todos los archivos y subcarpetas, use la máscara **"D:*"**.
- Si solo desea excluir archivos doc, use la máscara **"*.doc"**.
- Si el nombre del archivo ejecutable tiene un número determinado de caracteres (que varían) y solo conoce el primero en forma segura (por ejemplo, "D"), use el siguiente formato: **"D?????.exe"**. Los símbolos de interrogación reemplazan a los caracteres faltantes (desconocidos).

Ruta de acceso	Amenaza
C:\inetpub\logs\LogFiles*.log	
C:\inetpub\temp\IIS Temporary Compressed Files*.*	
C:\pagefile.sys	
C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess*.*	
C:\Program Files\Microsoft\Exchange Server\V15\FIP-FS*.*	
C:\Program Files\Microsoft\Exchange Server\V15\GroupMetrics*.*	
C:\Program Files\Microsoft\Exchange Server\V15\Logging\Calendar Repair Assist...	
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1628...	
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1628...	
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\IpFilter*.*	
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.*	

Agregar

Editar

Quitar

Aceptar

Cancelar

i NOTA

una amenaza dentro de un archivo no se detectará por el módulo de protección del sistema de archivos en tiempo real o módulo de exploración del equipo si dicho archivo cumple con los criterios para la exclusión de la exploración.

Columnas

Ruta: ruta a los archivos y las carpetas excluidos.

Amenaza: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo solo se excluirá de la exploración en lo que respecta a dicha amenaza. Si dicho archivo más tarde se infecta con otro código malicioso, el módulo antivirus lo detectará. Este tipo de exclusión puede usarse solamente para ciertos tipos de infiltraciones, y puede crearse ya sea en la ventana de alerta de amenazas que informa sobre la infiltración (haga clic en **Más información** y luego seleccione **Excluir de la detección**), o al hacer clic en **Herramientas > Cuarentena**, haciendo clic con el botón secundario sobre el archivo en cuarentena y luego seleccionando **Restaurar y excluir de la detección** desde el menú contextual.

Elementos de control

Agregar: excluye objetos de la detección.

Editar: le permite editar las entradas seleccionadas.

Quitar: quita las entradas seleccionadas.

4.2.6.1.1 Agregar o editar exclusiones

Esta ventana de diálogo permite agregar o editar exclusiones. Hay dos formas de hacerlo:

- al escribir la ruta hacia el objeto que se desea excluir,
- al seleccionarlo en la estructura con forma de árbol (clic en ... al final del campo de texto para examinar)

Si usa el primer método, se pueden emplear los caracteres globales descritos en la sección [Formato de las exclusiones](#).

4.2.6.1.2 Formato de las exclusiones

Puede usar caracteres globales para abarcar un grupo de archivos. Un signo de interrogación (?) representa un carácter único variable, mientras que un asterisco (*) representa una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos en una carpeta, escriba la ruta a la carpeta y use la máscara “*.*”.
- Para excluir un disco completo incluyendo todos los archivos y subcarpetas, use la máscara “D:*”.
- Si solo desea excluir archivos doc, use la máscara “*.doc”.
- Si el nombre del archivo ejecutable tiene un número determinado de caracteres (que varían) y solo conoce el primero en forma segura (por ejemplo, “D”), use el siguiente formato: “D?????.exe”. Los símbolos de interrogación reemplazan a los caracteres faltantes (desconocidos).

4.2.6.2 ThreatSense parámetros

ThreatSense es una tecnología conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. usa una combinación de la exploración del código, la emulación del código, las firmas genéricas y las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar varios flujos de datos simultáneamente, lo que maximiza la eficiencia y la tasa de detección. La tecnología ThreatSense también elimina con éxito los rootkits.

NOTA

para más detalles sobre la verificación de archivos de inicio, consulte [Exploración de arranque](#).

Las opciones de configuración del motor ThreatSense permiten especificar varios parámetros de exploración:

- los tipos de archivos y las extensiones que se van a explorar;
- la combinación de diversos métodos de detección;
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en **ThreatSense Configuración de los parámetros del motor** en la ventana de Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes escenarios de seguridad pueden requerir distintas configuraciones. Por ese motivo, ThreatSense puede configurarse en forma individual para cada uno de los siguientes módulos de protección:

- [Protección del transporte de correo electrónico](#)
- [Protección de la base de datos a petición](#)
- [Protección de la base de datos de correo electrónico](#)
- [Protección del sistema de archivos en tiempo real](#)
- [Exploración de Hyper-V](#)
- [Protección del sistema de archivos en tiempo real](#)
- [Exploración en estado inactivo](#)
- [Exploración en el inicio](#)
- [Protección de documentos](#)
- [Protección del cliente de correo electrónico](#)
- [Protección del acceso a la Web](#)
- [Exploración del equipo](#)

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

Objetos para explorar

Esta sección le permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

- **Memoria operativa:** explora en busca de amenazas que atacan la memoria operativa del sistema.
- **Sectores de inicio:** explora los sectores de inicio para detectar la presencia de virus en el MBR (Master Boot Record). En caso de una máquina virtual de Hyper-V, el MBR de su disco se explora en el modo solo lectura.
- **Archivos de correo electrónico:** el programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.
- **Archivos comprimidos:** el programa es compatible con las siguientes extensiones: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, entre muchas otras.
- **Archivos comprimidos de autoextracción:** los archivos comprimidos de autoextracción (SFX) son archivos comprimidos que no necesitan ningún programa de extracción especializado para descomprimirse.
- **Empaquetadores de tiempo de ejecución:** después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos comprimidos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

NOTA

En el caso de la protección de la base de datos del buzón de mensajes, los **Archivos de correo electrónico** como datos adjuntos (por ejemplo *.eml*) se exploran independientemente de la configuración bajo **Objetos para explorar**. Esto se debe a que el Servidor de Exchange analiza los datos adjuntos *.eml* antes de enviarlo a ESET Mail Security para que lo explore. El complemento VSAPI obtiene los archivos extraídos de los datos adjuntos del *.eml* en lugar de recibir el archivo *.eml* original.

Opciones de exploración

Seleccione los métodos usados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

- **Heurística:** la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por la base de datos de firmas de virus anterior. La desventaja es la probabilidad (muy reducida) de identificar los falsos positivos.
- **Heurística avanzada/ADN/Firmas inteligentes:** la heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que fueron creados con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Limpieza

La configuración de la desinfección determina el comportamiento del módulo de exploración durante la desinfección de los archivos infectados. Existen 3 niveles de desinfección:

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de advertencia y le permitirá al usuario que seleccione una acción. Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de detectar una infiltración.

Desinfección normal: el programa intentará desinfectar o eliminar el archivo infectado automáticamente basándose en una acción predefinida (dependiendo del tipo de infiltración). La detección y eliminación de un archivo infectado se marca con una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta en forma automática, el programa ofrece otras acciones que se pueden realizar. Ocurre lo mismo cuando no es posible completar una acción predefinida.

Desinfección estricta: el programa desinfectará o eliminará todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se le preguntará al usuario qué tipo de acción se debe realizar.

ADVERTENCIA

Si un archivo comprimido contiene uno o varios archivos infectados, existen dos opciones para tratarlo. En el modo estándar (Desinfección estándar), se eliminará el archivo comprimido completo cuando todos los archivos que incluya estén infectados. En el modo de **Desinfección estricta**, el archivo comprimido se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

IMPORTANTE

Si el host de Hyper-V no se está ejecutando en Windows Server 2008 R2, **Desinfección normal** y **Desinfección estricta** no son compatibles. La exploración de los discos de las máquinas virtuales se realiza en el modo solo lectura: **Sin desinfección**. Sin importar el nivel de desinfección seleccionado, la exploración siempre se realiza en el modo solo lectura.

Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de los parámetros de ThreatSense permite definir los tipos de [archivos a excluir de la exploración](#).

Otros

Cuando se configuran los valores de los parámetros del motor ThreatSense para una exploración del equipo a petición, las siguientes opciones en la sección **Otros** también están disponibles:

- **Explorar secuencias de datos alternativas (ADS):** las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección, camuflándose como secuencias de datos alternativas.
- **Realizar exploraciones en segundo plano con baja prioridad:** cada secuencia de exploración consume una cantidad determinada de recursos del sistema. Si se trabaja con los programas cuyo consumo de recursos constituye una carga importante para los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.
- **Registrar todos los objetos:** si se selecciona esta opción, el archivo de registro mostrará todos los archivos explorados, incluso los que no estén infectados. Por ejemplo, si se detecta una infiltración dentro de un archivo comprimido, el registro también incluirá en la lista los archivos no infectados de dicho archivo.
- **Habilitar la optimización inteligente:** cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración más favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de esos módulos específicos al efectuar una exploración.
- **Preservar el último acceso con su fecha y hora:** seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Configuración de los objetos

Configuración predeterminada del objeto

- **Tamaño máximo del objeto:** define el tamaño máximo de los objetos que se van a explorar. El módulo antivirus determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: *ilimitado*.
- **Tiempo máximo de exploración para el objeto (seg.):** define el valor máximo de tiempo para explorar un objeto. Si en esta opción se ingresó un valor definido por el usuario, el módulo antivirus detendrá la exploración de un objeto cuando haya transcurrido dicho tiempo, sin importar si finalizó la exploración. Valor predeterminado: *ilimitado*.

Configuración de la exploración de archivos comprimidos

Nivel de anidado de archivos comprimidos: especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: *10*.

Tamaño máximo del archivo incluido en el archivo comprimido: esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. Valor predeterminado: *ilimitado*.

NOTA

no se recomienda cambiar los valores predeterminados; en circunstancias normales, no existe ninguna razón para modificarlos.

4.2.6.2.1 Extensiones de archivos que no se analizarán

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de los parámetros de ThreatSense permite definir los tipos de archivos que se van a explorar.

En forma predeterminada, se exploran todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos de la exploración.

A veces es necesario excluir ciertos tipos de archivos cuando su exploración impide el funcionamiento correcto del programa que está usando ciertas extensiones. Por ejemplo, puede ser recomendable excluir las extensiones .edb, .eml y .tmp al usar los servidores de Microsoft Exchange.

Mediante el uso de los botones **Agregar** y **Quitar**, puede permitir o prohibir la exploración de extensiones de archivos específicas. Para agregar una nueva extensión a la lista, haga clic en **Agregar**, escriba la extensión en el campo en blanco y haga clic en **Aceptar**. Cuando selecciona **Ingresar múltiples valores**, puede agregar varias extensiones de archivo delimitadas por líneas, comas, o punto y coma. Cuando se habilita la selección múltiple, las extensiones se mostrarán en la lista. Seleccione una extensión de la lista y haga clic en **Quitar** para eliminar esa extensión de la lista. Si desea editar una extensión seleccionada, haga clic en **Editar**.

Se puede usar el símbolo especial “?” (signo de interrogación). El símbolo de interrogación representa cualquier símbolo.

NOTA

Para ver la extensión exacta (si hubiera) de un archivo en un sistema operativo de Windows, debe anular la selección de la opción **Ocultar las extensiones de los tipos de archivo conocidos** en **Panel de control > Opciones de carpeta > Ver** (pestaña) y aplicar este cambio.

4.2.6.2.2 Parámetros ThreatSense adicionales

Parámetros adicionales de ThreatSense para los nuevos archivos creados y modificados: la probabilidad de infección de los nuevos archivos creados o de los modificados es mayor al compararla con la correspondiente a los archivos existentes. Por ese motivo, el programa verifica esos archivos con parámetros adicionales de exploración. Junto con los métodos comunes de exploración basados en firmas, se usa la heurística avanzada, que puede detectar las nuevas amenazas antes del lanzamiento de la actualización de la base de datos de firmas de virus. Además de los nuevos archivos creados, la exploración se realiza en los archivos de autoextracción (.sfx) y los empaquetadores de tiempo de ejecución (archivos ejecutables comprimidos internamente). En forma predeterminada, los archivos comprimidos se exploran hasta el décimo nivel de anidado y se verifican independientemente de su tamaño real. Para modificar la configuración de la exploración de los archivos comprimidos, desactive **Configuración predeterminada para la exploración de archivos comprimidos**.

Para obtener más información acerca de los **Empaquetadores de tiempo de ejecución**, los **Archivos de autoextracción** y la **Heurística avanzada**, consulte la [Configuración de los parámetros del motor ThreatSense](#).

Parámetros adicionales de ThreatSense para los archivos ejecutados: en forma predeterminada, la [Heurística avanzada](#) se usa cuando se ejecutan los archivos. Cuando está habilitada, recomendamos firmemente mantener la [Optimización inteligente](#) y <%ELG%> habilitados para mitigar el impacto en el rendimiento del sistema.

4.2.6.2.3 Niveles de desinfección

La protección en tiempo real tiene tres niveles de desinfección (para acceder a las configuraciones de los niveles de desinfección, haga clic en **Parámetros ThreatSense** en la sección **Protección del sistema de archivos en tiempo real** y luego haga clic en **Desinfección**).

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de advertencia y le permitirá al usuario que seleccione una acción. Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de detectar una infiltración.

Desinfección normal: el programa intentará desinfectar o eliminar el archivo infectado automáticamente basándose en una acción predefinida (dependiendo del tipo de infiltración). La detección y eliminación de un archivo infectado se marca con una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta en forma automática, el programa ofrece otras acciones que se pueden realizar. Ocurre lo mismo cuando no es posible completar una acción predefinida.

Desinfección estricta: el programa desinfectará o eliminará todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se le preguntará al usuario qué tipo de acción se debe realizar.

ADVERTENCIA


si un archivo comprimido contiene uno o varios archivos infectados, existen dos opciones para tratarlo. En el modo estándar (Desinfección estándar), se eliminará el archivo comprimido completo cuando todos los archivos que incluya estén infectados. En el modo de **Desinfección estricta**, el archivo comprimido se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

IMPORTANTE

Si el host de Hyper-V no se está ejecutando en Windows Server 2008 R2, **Desinfección normal** y **Desinfección estricta** no son compatibles. La exploración de los discos de las máquinas virtuales se realiza en el modo solo lectura: **Sin desinfección**. Sin importar el nivel de desinfección seleccionado, la exploración siempre se realiza en el modo solo lectura.

4.2.6.2.4 Cuándo modificar la configuración de la protección en tiempo real

La protección del sistema de archivos en tiempo real es el componente más imprescindible para mantener un sistema seguro. Siempre sea precavido al modificar sus parámetros. Recomendamos modificar los parámetros únicamente en casos específicos.

Luego de la instalación de ESET Mail Security, todas las configuraciones se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restablecer la configuración predeterminada, haga clic en  junto a cada pestaña de la ventana (**Configuración avanzada > Equipo > Protección del sistema de archivos en tiempo real**).

4.2.6.2.5 Verificación de la protección en tiempo real

Para verificar que la protección en tiempo real se encuentra activa y es capaz de detectar virus, use un archivo de prueba de eicar.com. Este archivo de prueba es un archivo inofensivo, al que detectan todos los programas antivirus. El archivo fue creado por la empresa EICAR (Instituto Europeo para la Investigación de los Antivirus Informáticos, por sus siglas en inglés) para comprobar la eficacia de los programas antivirus. El archivo está disponible para su descarga desde <http://www.eicar.org/download/eicar.com>

4.2.6.2.6 Qué hacer si la protección en tiempo real no funciona

En esta sección, se describirán problemas que se pueden presentar al usar la protección en tiempo real y se indicará cómo resolverlas.

La protección en tiempo real está deshabilitada

Si un usuario deshabilitó la protección en tiempo real sin darse cuenta, será necesario volver a activarla. Para reactivar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa durante el inicio del sistema, es posible que se deba a que **Iniciar automáticamente la protección del sistema de archivos en tiempo real** no está seleccionada. Para habilitar esta opción, vaya a Configuración avanzada (F5) y haga clic en **Equipo > Protección del sistema de archivos en tiempo real > Básico** en la sección **Configuración avanzada**. Asegúrese de que **Iniciar automáticamente la protección del sistema de archivos en tiempo real** esté activado.

Si la protección en tiempo real no detecta ni desinfecta infiltraciones

Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si están habilitados dos escudos de protección en tiempo real al mismo tiempo, es posible que entren en conflicto. Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa durante el inicio del sistema (e **Iniciar automáticamente la protección del sistema de archivos en tiempo real** está habilitada), es posible que se deba a la existencia de conflictos con otros programas. Para obtener asistencia para resolver este problema, comuníquese con Atención al cliente de ESET.

4.2.6.2.7 Envío

El usuario tiene la posibilidad de seleccionar la manera en que los archivos y la información estadística se enviarán a ESET. Seleccione la opción **Por medio de ESET Remote Administrator o directamente a ESET** para que se envíen los archivos y las estadísticas por cualquier medio disponible. Seleccione la opción **Por medio de ESET Remote Administrator** para enviar los archivos y las estadísticas al servidor de administración remota, que luego se asegurará de que se reenvíen al laboratorio de amenazas de ESET. Si se encuentra seleccionada la opción **Directamente a ESET**, todos los archivos sospechosos y la información estadística se enviarán al laboratorio de virus de ESET directamente desde el programa.

Cuando hay archivos pendientes para su envío, el botón **Enviar ahora** estará activo. Haga clic en el botón para enviar los archivos y la información estadística de inmediato.

Seleccione la opción **Habilitar registro** para crear un registro con los archivos y la información estadística de los envíos.

4.2.6.2.8 Estadísticas

El sistema de alerta temprana ThreatSense.Net recopila información anónima sobre el equipo en relación con las nuevas amenazas detectadas. Esta información puede incluir el nombre de la infiltración, la fecha y la hora en que fue detectada, la versión del producto de seguridad de ESET, la versión del sistema operativo y la configuración de la ubicación. En general, las estadísticas se envían a los servidores de ESET una o dos veces por día.

A continuación se muestra un ejemplo de un paquete estadístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Argentina"
# language="ESPAÑOL"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Cuándo enviar: permite definir cuándo se enviará la información estadística. Si elige enviar **lo antes posible**, la información estadística se enviará de inmediato tras su creación. Esta configuración es apropiada si existe una conexión permanente a Internet. Si se encuentra seleccionada la opción **Durante la actualización**, toda la información estadística se enviará en forma masiva durante la siguiente actualización.

4.2.6.2.9 Archivos sospechosos

La pestaña **Archivos sospechosos** permite configurar la manera en que las amenazas se envían al laboratorio de amenazas de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio de amenazas para su análisis. Si se trata de una aplicación maliciosa, se agregará su detección en la siguiente actualización de firmas de virus.

Se puede configurar el envío de archivos para que se realice en forma automática o seleccionar la opción **Preguntar antes de enviar** si desea conocer qué archivos se prepararon para enviar para su análisis, y confirmar el envío.

Si no desea que se envíe ningún archivo, seleccione la opción **No enviar para su análisis**. Si selecciona no enviar los archivos para su análisis, no afectará el envío de la información estadística, lo que se configura en una sección aparte (ver la sección [Estadísticas](#)).

Cuándo enviar: de forma predeterminada, se selecciona la opción **Lo antes posible** para enviar los archivos sospechosos al laboratorio de amenazas de ESET. Es la opción recomendada si hay una conexión permanente a Internet disponible y los archivos sospechosos se pueden enviar sin demoras. Seleccione la opción **Durante la actualización** para que los archivos sospechosos se carguen a ThreatSense.Net durante la siguiente actualización.

Filtro de exclusión: el filtro de exclusión permite excluir ciertos archivos o carpetas del envío. Por ejemplo, quizá resulte útil excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen en forma predeterminada (.doc, etc.). Si lo desea, puede agregar archivos a la lista de archivos excluidos.

Correo electrónico de contacto: puede enviar su **Correo electrónico de contacto (opcional)** junto con los archivos sospechosos, así podrá usarse para contactarlo en caso de que se requiera información adicional para el análisis. Recuerde que no recibirá ninguna respuesta de ESET a menos que se necesite información adicional.

4.2.7 Exploración del equipo y exploración de Hyper-V a petición

Esta sección contiene las opciones para seleccionar los parámetros de exploración.

i NOTA

Este selector de perfiles de exploración se aplica a la exploración del equipo y la [Exploración de Hyper-V a petición](#).

Perfil seleccionado: es un grupo específico de parámetros usado por el módulo de exploración a petición. Para crear uno nuevo, haga clic en **Editar** junto a la **Lista de perfiles**.

Si solo desea explorar un objeto específico, puede hacer clic en **Editar** junto a **Objetos para explorar** y elegir una opción del menú desplegable o puede seleccionar los objetos específicos desde la estructura (de árbol) de la carpeta.

La ventana de objetos para explorar le permite definir qué objetos (memoria, unidades, sectores, archivos y carpetas) se exploran en busca de infiltraciones. Seleccione los objetos desde la estructura con forma de árbol, que incluye la lista de todos los dispositivos disponibles en el equipo. El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

- **Por configuración de perfil:** selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles:** selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales:** selecciona todos los discos rígidos del sistema.
- **Unidades de red:** selecciona todas las unidades de red asignadas.
- **Carpetas compartidas:** selecciona todas las carpetas compartidas en el servidor local.
- **Sin selección:** cancela todas las selecciones.

Haga clic en [ThreatSense parámetros](#) para modificar los parámetros de exploración (por ejemplo, los métodos de detección) para el explorador del equipo a petición.

4.2.7.1 Ejecución de la exploración personalizada y exploración Hyper-V

Si solo desea explorar un objeto específico, puede usar la herramienta de Exploración personalizada al hacer clic en **Exploración del equipo > Exploración personalizada** y, luego, seleccione una opción del menú desplegable **Objetos para explorar**, o bien seleccione los objetos específicos desde la estructura (de árbol) de la carpeta.

i NOTA

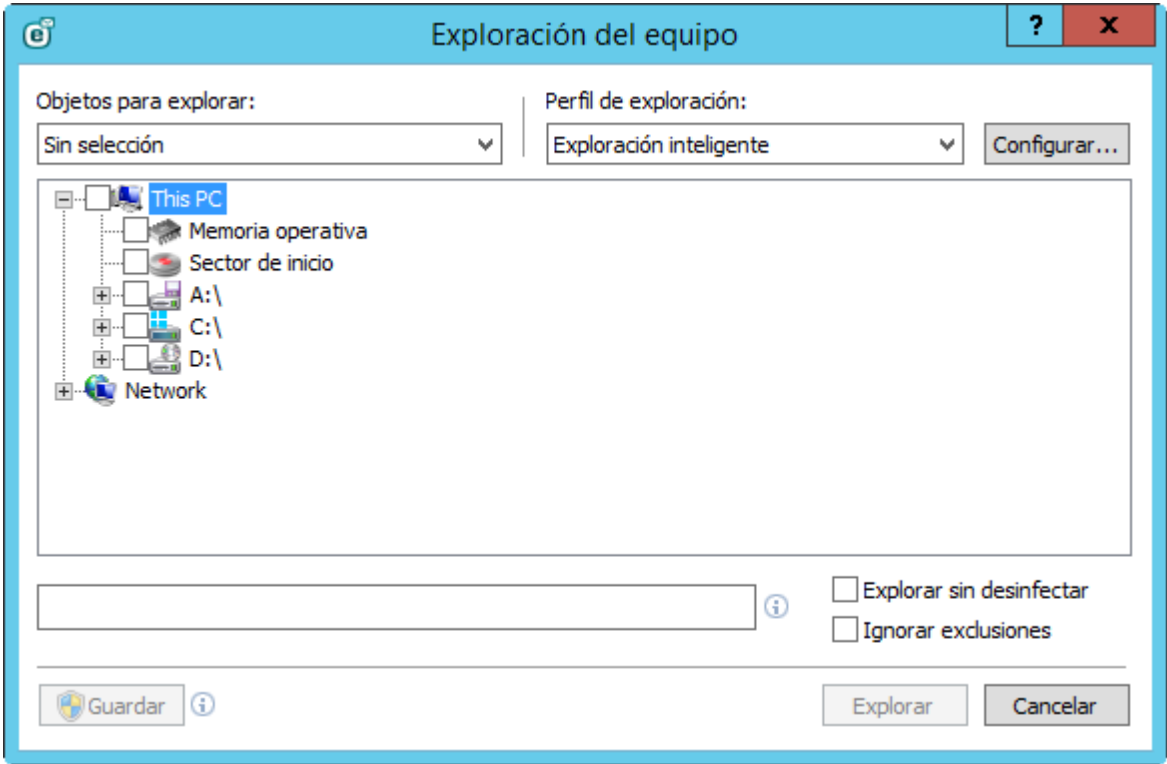
Este selector de exploración de objetos aplica a la Exploración personalizada y [Exploración Hyper-V](#).

La ventana de objetos para explorar le permite definir qué objetos (memoria, unidades, sectores, archivos y carpetas) se exploran en busca de infiltraciones. Seleccione los objetos desde la estructura con forma de árbol, que incluye la lista de todos los dispositivos disponibles en el equipo. El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

- **Por configuración de perfil:** selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles:** selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales:** selecciona todos los discos rígidos del sistema.
- **Unidades de red:** selecciona todas las unidades de red asignadas.
- **Carpetas compartidas:** selecciona todas las carpetas compartidas en el servidor local.
- **Sin selección:** cancela todas las selecciones.

Para ir rápidamente hasta un objeto para explorar o para agregar en forma directa un objeto para explorar (carpeta o archivos), ingréselo en el campo vacío debajo de la lista de carpetas. Esta acción solo será posible si no se seleccionó ningún objeto para explorar en la estructura con forma de árbol y el menú **Objetos para explorar** está configurado en **Sin selección**.

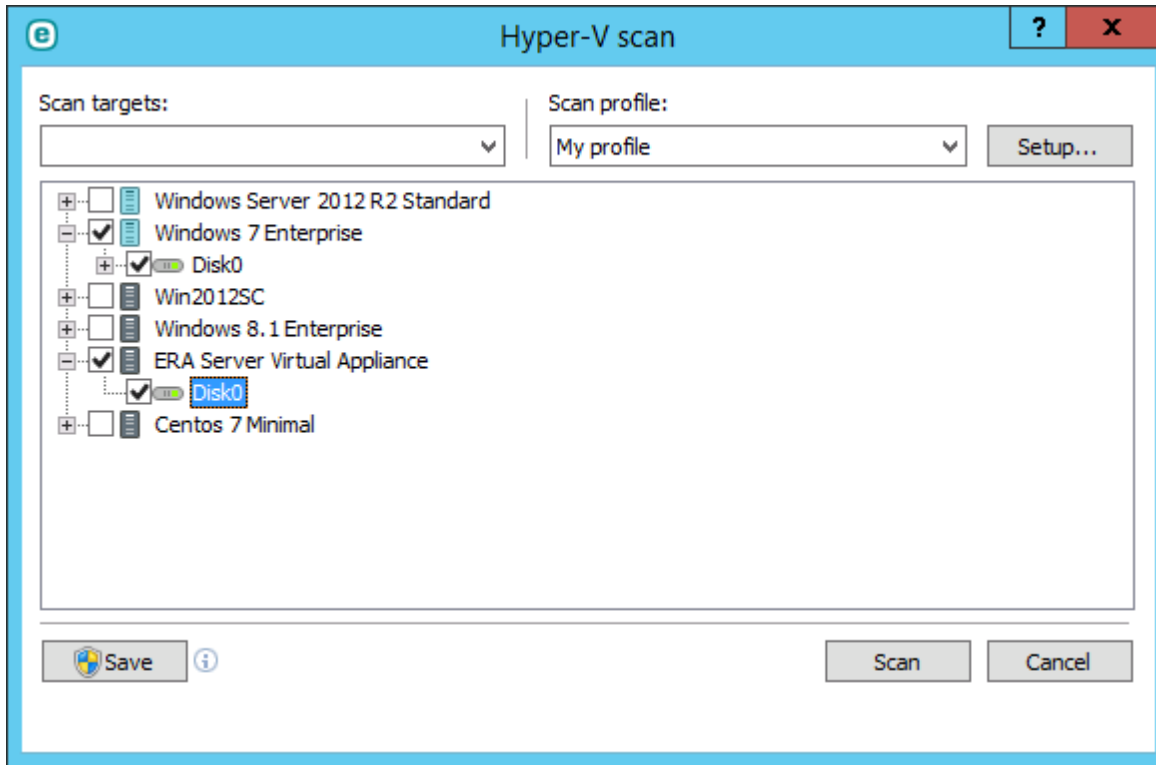
Ventana emergente **Exploración personalizada**:



Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Esto es útil cuando solo desea obtener un resumen de si hay elementos infectados y ver los detalles acerca de estas infecciones, si las hay. Además, puede elegir de entre tres niveles de desinfección al hacer clic en **Configuración > ParámetrosThreatSense > Desinfección**. La información sobre la exploración se guarda en un registro de exploración.

Cuando selecciona **Ignorar exclusiones**, le permite realizar una exploración mientras ignora [exclusiones](#) que de otro modo se aplicarían.

Ventana emergente **Exploración de Hyper-V** (consulte [Exploración Hyper-V](#) para obtener más información):



En el menú desplegable **Perfil de exploración**, puede elegir un perfil que podrá usar con los objetos para explorar seleccionados. El perfil predeterminado es **Exploración inteligente**. Hay otros dos perfiles de exploración predefinidos denominados **Exploración profunda** y **Exploración del menú contextual**. Estos perfiles de exploración usan diferentes [parámetros del motor ThreatSense](#). Haga clic en el botón **Configurar...** para establecer detalladamente el perfil de exploración seleccionado desde el menú de perfiles de exploración. Las opciones disponibles se describen en la sección **Otros** en la [Configuración de los parámetros del motor ThreatSense](#).

Guardar: para guardar los cambios realizados en su selección de objetos, incluyendo las selecciones hechas dentro de la carpeta con estructura en forma de árbol.

Haga clic en **Explorar** para ejecutar la exploración con los parámetros personalizados establecidos.

Explorar como administrador permite ejecutar la exploración desde una cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene los privilegios necesarios para acceder a los archivos apropiados que se van a explorar. Tenga en cuenta que este botón no está disponible si el usuario actual no puede realizar operaciones UAC como administrador.

4.2.7.2 Progreso de la exploración

La ventana de progreso de la exploración muestra el estado actual de la exploración junto con información sobre la cantidad detectada de archivos con códigos maliciosos.

Exploración inteligente

?

Progreso de la exploración

Amenazas detectadas: 0

C:\Documents and Settings\All Users\ESET\ESET Mail Security\updfiles\em009_64_IO.nup

Registro

C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat - error al ...
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Temp\2\BCG8558.tmp - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryS...
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Internet Explorer\Recovery\High\Active\{4EA84636...
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Internet Explorer\Recovery\High\Active\{4EA84637...
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\UsrClass.dat - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\UsrClass.dat.LOG1 - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\UsrClass.dat.LOG2 - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\WebCacheLock.dat - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\Notifications\WPNPRMRY.tmp - error al ...
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\WebCache\V01.log - error al abrir
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Microsoft\Windows\WebCache\WebCacheV01.dat - error al a...
C:\Documents and Settings\Administrator.CONTOSO\Local Settings\Temp\2\BCG8558.tmp - error al abrir

☒ Desplazarse por el registro de exploración

Detener

Pausar

NOTA
es común que algunos archivos, como los archivos protegidos por contraseña o los que usa el sistema de manera exclusiva (habitualmente, archivos *pagefile.sys* y ciertos archivos de registro), no se puedan explorar.

Progreso de la exploración: la barra de progreso muestra el porcentaje de objetos ya explorados en comparación con los objetos que aún faltan explorar. El estado de progreso de la exploración proviene de la cantidad total de objetos incluidos en la exploración.

Destino: el nombre del objeto actualmente explorado y su ubicación.

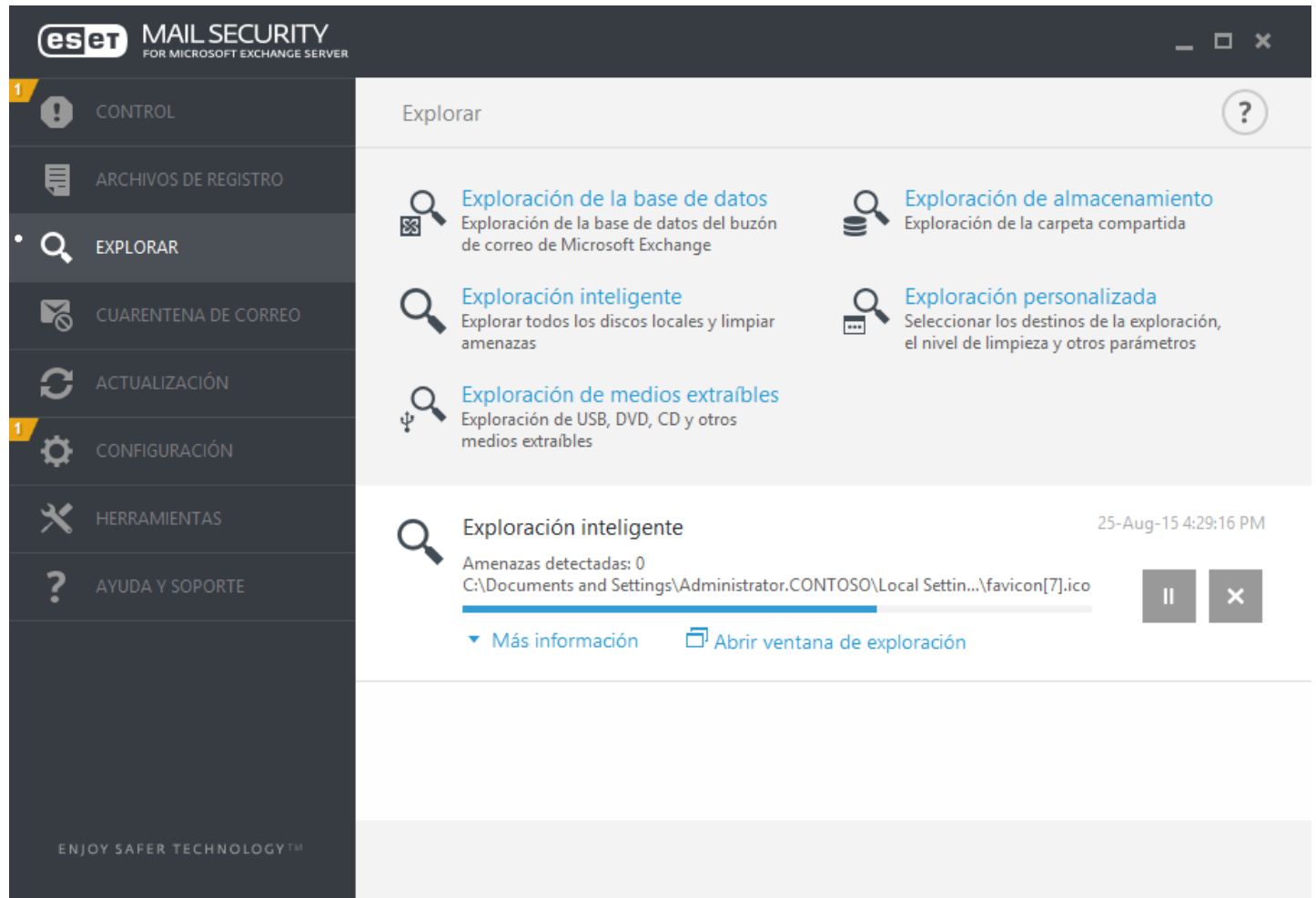
Amenazas encontradas: muestra el número total de amenazas encontradas durante una exploración.

Pausar: pone una exploración en pausa.

Reanudar: esta opción es visible cuando el progreso de la exploración está en pausa. Haga clic en Reanudar para proseguir con la exploración.

Detener: finaliza la exploración.

Desplazarse por el registro de exploración: si la opción está habilitada, el registro de exploración se desplazará hacia abajo automáticamente a medida que las nuevas entradas se van agregando para que sean visibles las más recientes.



Puede hacer clic en **Más información** durante el progreso de la exploración para ver detalles como el **Usuario** que ejecutó dicho proceso de exploración desde GUI, una cantidad de **Objetos explorados** y la **Duración** de la exploración. Si se está ejecutando una **Exploración de la base de datos** a petición, muestra al usuario quién ejecutó la exploración, no la Cuenta de exploración de la base de datos real que se está usando para conectar a EWS (Servicios web de Exchange) durante el proceso de exploración.

4.2.7.3 Administrador de perfiles

El administrador de perfiles se usa en dos partes de ESET Mail Security: en la sección **Exploración del equipo a petición** y en **Actualización**.

Exploración del equipo a petición

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración usada regularmente.

Para crear un nuevo perfil, abra la ventana de configuración Avanzada (F5) y haga clic en **Equipo > Exploración del**

equipo a petición y luego **Editar** junto a la **Lista de perfiles**. El menú desplegable **Perfil seleccionado** enumera los perfiles de exploración existentes. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección [Configuración de los parámetros del motor ThreatSense](#), donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

Ejemplo: Suponga que desea crear su propio perfil de exploración y la configuración de la exploración inteligente es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y, además, quiere aplicar una **Desinfección estricta**. Ingrese el nombre de su nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione su nuevo perfil desde el menú desplegable **Perfil seleccionado** y ajuste los parámetros restantes para cumplir con sus requisitos, y haga clic en **Aceptar** para guardar su nuevo perfil.

Actualización

El editor de perfiles, en la sección de configuración de la actualización, permite a los usuarios crear nuevos perfiles de actualización. Solamente es necesario crear perfiles de actualización personalizados si su equipo usa varios medios para conectarse a los servidores de actualización.

Un ejemplo es un equipo portátil que normalmente se conecta a un servidor local (mirror) desde la red local, pero que descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (durante un viaje de negocios) puede usar dos perfiles: el primero para conectarse al servidor local; el otro para conectarse a los servidores de ESET. Una vez configurados estos perfiles, navegue a **Herramientas > Tareas programadas** y edite los parámetros de las tareas de actualización. Designe un perfil como principal y el otro como secundario.

Perfil seleccionado: el perfil de actualización usado actualmente. Para cambiarlo, elija un perfil del menú desplegable.

Lista de perfiles: cree perfiles nuevos o edite perfiles de actualización.

4.2.7.4 Objetos para explorar

La ventana de objetos para explorar le permite definir qué objetos (memoria, unidades, sectores, archivos y carpetas) se exploran en busca de infiltraciones. Seleccione los objetos desde la estructura con forma de árbol, que incluye la lista de todos los dispositivos disponibles en el equipo. El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

- **Por configuración de perfil:** selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles:** selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales:** selecciona todos los discos rígidos del sistema.
- **Unidades de red:** selecciona todas las unidades de red asignadas.
- **Carpetas compartidas:** selecciona todas las carpetas compartidas en el servidor local.
- **Sin selección:** cancela todas las selecciones.

4.2.7.5 Pausar la exploración programada

Se puede posponer la exploración programada. Establezca un valor para la opción **Detener exploraciones programadas en (min)**, si desea posponer la exploración del equipo.

4.2.8 Exploración en estado inactivo

Puede habilitar el explorador en estado inactivo en **Configuración avanzada** bajo **Equipo > Exploración en estado inactivo > Básico**. Configure el interruptor junto a **Habilitar la exploración en estado inactivo** en Encendido para habilitar esta característica. Cuando el equipo está en estado inactivo, se realiza una exploración silenciosa en todas las unidades locales del equipo.

De forma predeterminada, la exploración de estado inactivo no se accionará cuando el equipo (portátil) está funcionando con la energía de la batería. Puede anular esta configuración al seleccionar la casilla de verificación junto a **Ejecutar incluso si el equipo recibe alimentación de la batería** en la Configuración avanzada.

Encienda el interruptor **Habilitar la creación de registros** en la Configuración avanzada para registrar el resultado de

la exploración del equipo en la sección [Archivos de registro](#) (desde la ventana principal del programa haga clic en **Herramientas > Archivos de registro** y seleccione **Exploración del equipo** en el menú desplegable **Registro**).

La detección en estado inactivo se ejecutará cuando su equipo se encuentre en los siguientes estados:

- Pantalla apagada o protector de pantalla
- Bloqueo de equipo
- Cierre de sesión de usuario

Haga clic en [ThreatSense parámetros](#) para modificar los parámetros de exploración (por ejemplo, los métodos de detección) para el explorador en estado inactivo.

4.2.9 Exploración en el inicio

En forma predeterminada, la exploración automática de archivos durante el inicio del sistema se realizará durante el inicio del sistema y durante la actualización de la base de datos de firmas de virus. Esta exploración es controlada por la [Configuración y las tareas programadas](#).

Las opciones de exploración en el inicio son parte de la tarea programada de la **Verificación de archivos de inicio del sistema**. Para modificar Configuraciones de exploración en el inicio, navegue a **Herramientas > Tareas programadas**, haga clic en **Exploración automática de archivos durante el inicio del sistema** y luego en **Editar**. En el último paso, aparecerá la ventana [Exploración automática de archivos durante el inicio del sistema](#) (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas sobre la creación y administración de tareas programadas, consulte la [Creación de tareas nuevas](#).

4.2.9.1 Verificación de archivos de inicio automática

Al crear una tarea programada de verificación de archivos de inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Nivel de exploración** especifica la profundidad de la exploración para la ejecución de archivos al inicio del sistema. Los archivos se organizan en orden ascendente de acuerdo con el siguiente criterio:

- **Solo los archivos más frecuentemente usados** (los archivos menos explorados)
- **Archivos de uso más frecuente**
- **Archivos usados habitualmente**
- **Archivos poco usados**
- **Todos los archivos registrados** (la mayoría de archivos explorados)

También se incluyen dos grupos específicos de **Nivel de exploración**:

- **Archivos que se ejecutan antes del registro del usuario:** contiene archivos de las ubicaciones a las que puede accederse sin que el usuario se registre (incluye casi todas las ubicaciones de inicio tales como servicios, objetos del ayudante de exploración, winlogon notify, entradas de las tareas programadas de ventanas, dll conocidos, etc.).
- **Archivos que se ejecutan después del registro del usuario:** contiene archivos de las ubicaciones a las que puede accederse solo después de que un usuario se registre (incluye archivos que solo se ejecutan para un usuario específico, por lo general archivos en `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Las listas de archivos a escanear son fijas para cada grupo antes mencionado.

Prioridad de exploración: el nivel de prioridad usado para determinar cuándo se iniciará una exploración:

- **Normal:** en una carga promedio del sistema,
- **Inferior:** en una carga baja del sistema,
- **Más baja:** cuando la carga del sistema es lo más baja posible,
- **Cuando está inactivo:** la tarea se realizará solo cuando el sistema esté inactivo.

4.2.10 Medios extraíbles

ESET Mail Security proporciona la exploración automática de los medios extraíbles (CD/DVD/USB). Este módulo le permite explorar los medios insertados. Resulta útil si el administrador del equipo desea prevenir que los usuarios usen los medios extraíbles con contenido no solicitado.

Acción a realizar después de insertar un medio extraíble : seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el equipo (CD/DVD/USB). Si se selecciona **Mostrar las opciones de exploración**, se mostrará una notificación que le permite elegir una acción deseada:

- **No explorar**: no se realizará ninguna acción y se cerrará la ventana **Se detectó un nuevo dispositivo**.
- **Exploración automática del dispositivo**: se llevará a cabo una exploración del equipo a petición en los dispositivos de medios extraíbles insertados.
- **Mostrar las opciones de exploración**: abre la sección de configuración de medios extraíbles.

Cuando se inserten los medios extraíbles, se mostrará el siguiente cuadro de diálogo:

- **Explorar ahora**: desencadenará la exploración de los medios extraíbles.
- **Explorar más tarde**: se pospone la exploración de los medios extraíbles.
- **Configuración**: abre la Configuración avanzada.
- **Usar siempre la opción seleccionada**: de seleccionarse, se llevará a cabo la misma acción cuando se inserte un medio extraíble en el futuro.

Además, ESET Mail Security presenta la funcionalidad de Control del dispositivo, que le permite definir las reglas para el uso de dispositivos externos en un equipo determinado. Se pueden encontrar más detalles sobre el Control del dispositivo en la sección [Control del dispositivo](#).

4.2.11 Protección de documentos

La característica de protección de documentos explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer, por ejemplo, los elementos ActiveX de Microsoft. La protección de documentos proporciona un nivel de protección adicional a la protección del sistema de archivos en tiempo real. Puede deshabilitarse para mejorar el rendimiento en los sistemas que no están expuestos a un alto volumen de documentos de Microsoft Office.

- La opción **Integrar al sistema** activa el sistema de protección. Para modificar esta opción, presione F5 para abrir la ventana de configuración Avanzada y haga clic en **Equipo > Protección de documentos** en el árbol de configuración Avanzada.
- Consulte [Threatsense parámetros](#) para obtener más información sobre la configuración de la Protección de documentos.

Esta función se activa por medio de las aplicaciones que usan Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y posterior, o Microsoft Internet Explorer 5.0 y posterior).

4.2.12 HIPS

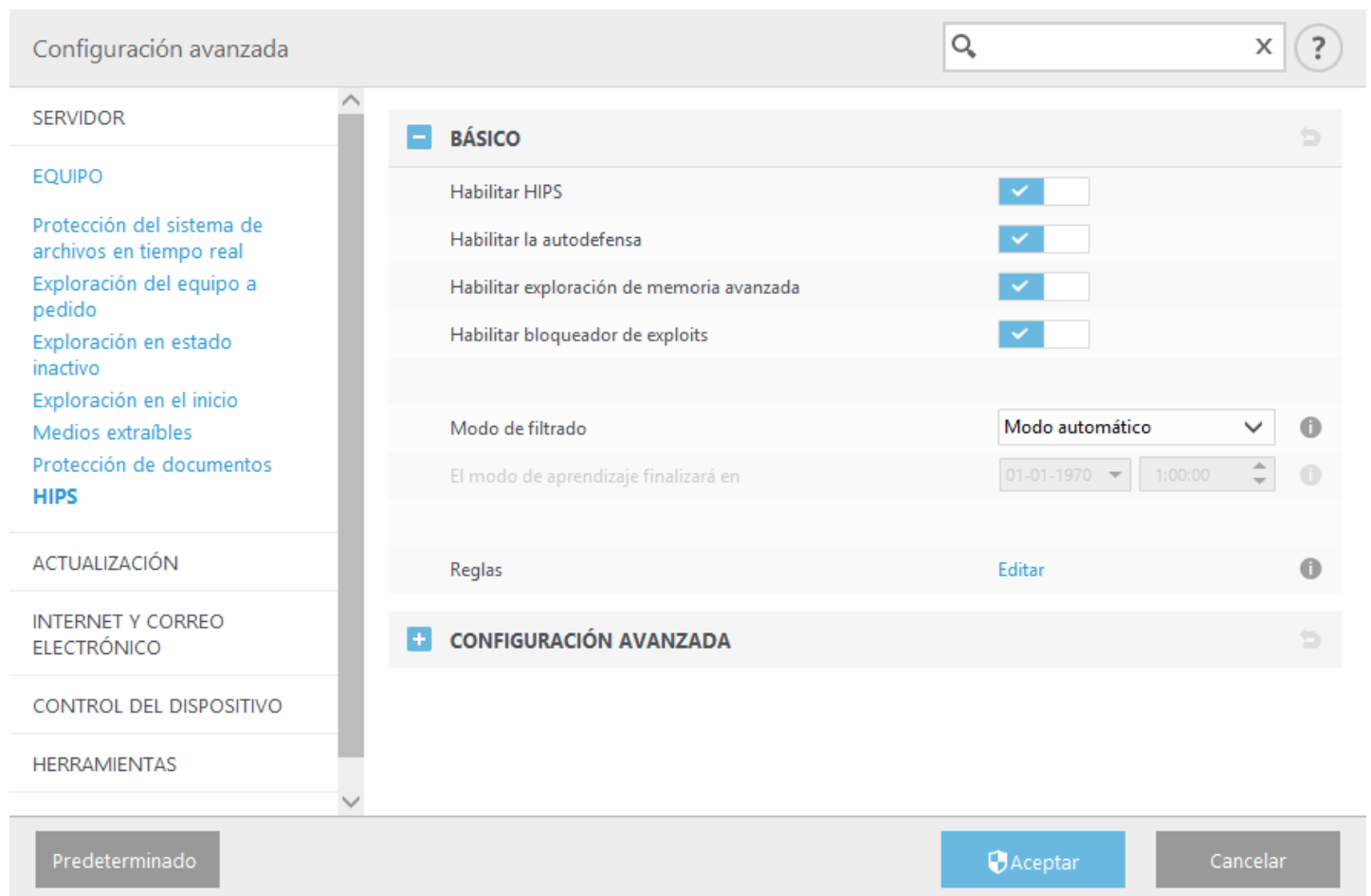


ADVERTENCIA

las modificaciones de la configuración del HIPS deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de HIPS puede llevar a la inestabilidad del sistema.

El **Sistema de prevención de intrusiones basado en el host (HIPS)** protege su sistema de malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS usa el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro. El HIPS es independiente de la protección del sistema de archivos en tiempo real y no es un firewall; solo monitorea los procesos activos en el sistema operativo.

Las configuraciones del HIPS se pueden encontrar en **Configuración avanzada (F5) > Equipo > HIPS**. El estado del HIPS (habilitado/deshabilitado) se muestra en la ventana principal del programa de ESET Mail Security, en el panel **Configuración**, del lado derecho de la sección **Equipo**.



ESET Mail Security cuenta con tecnología integrada de *Autodefensa* que evita que el software malicioso dañe o deshabilite la protección antivirus y antispyware, por lo que puede estar seguro de que su sistema permanece protegido constantemente. Los cambios en la configuración **Habilitar HIPS** y **Habilitar SD (Autodefensa)** se aplican luego del reinicio del sistema operativo Windows. La deshabilitación del sistema **HIPS** completo también requiere reiniciar el equipo.

La **Exploración de memoria avanzada** trabaja en conjunto con el Bloqueador de exploits para fortalecer la protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. La exploración de memoria avanzada está habilitada en forma predeterminada. Obtenga más información sobre este tipo de protección en el [glosario](#).

Bloqueador de exploits está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits está habilitado en forma predeterminada. Obtenga más información sobre este tipo de protección en el [glosario](#).

El filtrado se puede realizar en uno de los siguientes cuatro modos:

- **Modo automático:** las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las reglas predefinidas que protegen su sistema.
- **Modo inteligente:** se notificará al usuario solo en caso de eventos muy sospechosos.
- **Modo interactivo:** el programa le solicitará al usuario que confirme las operaciones.
- **Modo basado en políticas:** las operaciones están bloqueadas.
- **Modo de aprendizaje:** las operaciones están habilitadas y se crea una regla luego de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el Modo de aprendizaje en el menú desplegable del modo de filtrado de HIPS, la configuración del modo de aprendizaje finalizará cuando esté disponible. Seleccione el tiempo durante el cual desea activar el modo de aprendizaje (el tiempo máximo es de 14 días). Cuando el

tiempo especificado haya pasado, se le solicitará que edite las reglas creadas por HIPS mientras estuvo en el modo de aprendizaje. También puede elegir un modo de filtrado diferente, o posponer la decisión y continuar usando el modo de aprendizaje.

El sistema HIPS monitorea los sucesos dentro del sistema operativo y reacciona consecuentemente en función de reglas similares a las usadas por el firewall personal. Haga clic en **Editar** para abrir la ventana de administración de reglas de HIPS. Allí podrá seleccionar, crear, editar o eliminar reglas. Encontrará más detalles sobre la creación de reglas y las operaciones del sistema HIPS en el capítulo [Edición de una regla](#).

Si la acción predeterminada para una regla está configurada para Preguntar, una ventana de diálogo aparecerá cada vez que se active la regla. Puede elegir **Bloquear** o **Permitir** la operación. Si no elige una acción en el tiempo dado, se seleccionará una nueva acción en función de las reglas.

La ventana de diálogo le permite crear una regla en función de cualquier acción nueva que el HIPS detecte para, posteriormente, definir las condiciones mediante las cuales se permitirá o se bloqueará dicha acción. Se puede acceder a las configuraciones para los parámetros exactos al hacer clic en **Mostrar opciones**. Las reglas creadas de esta forma se consideran equivalentes a las creadas manualmente. En consecuencia, la regla creada desde una ventana de diálogo puede ser menos específica que la que activa la ventana de diálogo. Esto significa que, después de crear dicha regla, la misma operación puede activar la misma ventana.

Recordar la acción temporalmente para este proceso hace que la acción (**Permitir/Bloquear**) se use hasta que haya un cambio de reglas o de modo de filtrado, una actualización de módulo del HIPS o un reinicio del sistema. Las reglas temporales se eliminarán después de cualquiera de estas tres acciones.

4.2.12.1 Reglas HIPS

Esta ventana le brinda una visión general de las reglas HIPS existentes.

Columnas

Regla: nombre de la regla definido por el usuario o elegido automáticamente.

Habilitada: desactive este interruptor si desea conservar la regla en la lista pero no quiere usarla.

Acción: la regla especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo bajo las condiciones adecuadas.

Orígenes: la regla solo se usará si una aplicación o un número de aplicaciones accionan el evento.

Destinos: la regla solo se usará si la operación se relaciona con un archivo, una aplicación o una entrada de registro específicos.

Registro: si activa esta opción, la información sobre esta regla se incluirá en el [registro de HIPS](#).

Notificar: si se acciona un evento, aparece una ventana emergente pequeña en la esquina inferior derecha.

Elementos de control

Agregar: crea una regla nueva.

Editar: le permite editar las entradas seleccionadas.

Quitar: quita las entradas seleccionadas.

Reglas HIPS

Regla	Habilitar	Acción	Fuentes	Destinos	Registrar	No
Без имени	<input checked="" type="checkbox"/>	Permitir		Aplicaciones, Registro	<input type="checkbox"/>	<input type="checkbox"/>

<

III

>

Agregar

Editar

Quitar

Aceptar

Cancelar

4.2.12.1.1 Configuración de reglas HIPS

- **Nombre de la regla:** nombre de la regla definido por el usuario o elegido automáticamente.
- **Acción:** la regla especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo bajo las condiciones adecuadas.

Operaciones que afectan: debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se usará para este tipo de operación y para el destino seleccionado.

- **Archivos:** la regla solo se usará si la operación está relacionada con este destino. Seleccione Archivos específicos en el menú desplegable y haga clic en Agregar para agregar carpetas o archivos, o puede seleccionar Todos los archivos en el menú desplegable para agregar todas las aplicaciones.
- **Aplicaciones:** la regla solo se usará cuando esta aplicación o estas aplicaciones accionen el suceso. Seleccione Aplicaciones específicas en el menú desplegable y haga clic en Agregar para agregar carpetas o archivos, o puede seleccionar Todas las aplicaciones en el menú desplegable para agregar todas las aplicaciones.
- **Entradas de registro:** la regla solo se usará si la operación está relacionada con este destino. Seleccione Entradas específicas en el menú desplegable y haga clic en Agregar para agregar carpetas o archivos, o puede seleccionar Todas las entradas en el menú desplegable para agregar todas las aplicaciones.
- **Habilitada:** desactive este interruptor si desea conservar la regla en la lista pero no quiere usarla.
- **Registro:** si activa esta opción, la información sobre esta regla se incluirá en el [registro de HIPS](#).
- **Notificar al usuario:** cuando se acciona un suceso, aparece una ventana emergente pequeña en la esquina inferior derecha.

La regla está compuesta por partes que describen las condiciones que la accionan:

Aplicaciones de origen: la regla solo se usará si esta aplicación o estas aplicaciones accionan el evento. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todas las aplicaciones** del menú desplegable para agregar todas las aplicaciones.

Archivos: la regla solo se usará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas las aplicaciones.

Aplicaciones: la regla solo se usará si la operación está relacionada con este destino. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Entradas de registro: la regla solo se usará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

Descripciones de las operaciones más importantes:

Operaciones de archivos

- **Eliminar el archivo:** la aplicación pide permiso para eliminar el archivo de destino.
- **Escribir en el archivo:** la aplicación pide permiso para escribir en el archivo de destino.
- **Acceso directo al disco:** la aplicación está intentando leer el disco o escribir en él de una forma que no es la estándar, lo que evade los procedimientos comunes de Windows. Esto puede provocar que se modifiquen los archivos sin haber aplicado las reglas correspondientes. Esta operación puede haberse generado por malware que intenta evadir la detección, un software de creación de copias de seguridad que intenta hacer una copia exacta del disco, o un administrador de particiones que intenta reorganizar los volúmenes de disco.
- **Instalar enlace global:** se refiere al llamado de la función SetWindowsHookEx de la biblioteca MSDN.
- **Cargar controlador:** instalación y carga de controladores en el sistema.

Operaciones de la aplicación

- **Depurar otra aplicación:** adjuntar un depurador al proceso. Cuando se depura una aplicación, es posible ver y modificar muchos detalles de su conducta, así como acceder a sus datos.
- **Interceptar eventos desde otra aplicación:** la aplicación de origen está intentando capturar eventos dirigidos a una aplicación específica (por ejemplo, un keylogger que intenta capturar eventos del navegador).
- **Finalizar/suspender otra aplicación:** suspende, reanuda o termina un proceso (se puede acceder directamente desde el Explorador de procesos o el Panel de procesos).
- **Iniciar una aplicación nueva:** inicio de aplicaciones o procesos nuevos.
- **Modificar el estado de otra aplicación:** la aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar un código en su nombre. Esta funcionalidad puede resultar útil para proteger una aplicación esencial mediante su configuración como aplicación de destino en una regla que bloquee el uso de dicha operación.

Operaciones de registros

- **Modificar la configuración del inicio:** cualquier cambio en la configuración que defina qué aplicaciones se ejecutarán durante el inicio de Windows. Pueden encontrarse, por ejemplo, al buscar la clave Run en el registro de Windows.
- **Eliminar del registro:** eliminar una clave de registro o su valor.
- **Volver a nombrar la clave de registro:** volver a nombrar claves de registros.
- **Modificar el registro:** crear nuevos valores de claves de registro, modificar los valores existentes, cambiar datos de lugar en el árbol de la base de datos o configurar derechos de usuarios o de grupos para las claves de registro.

i NOTA

puede usar caracteres globales con ciertas restricciones al ingresar un destino. En lugar de usar una clave específica, se puede usar el símbolo * (asterisco) en las rutas del registro. Por ejemplo, `HKEY_USERS*\software` puede significar `HKEY_USER\.default\software` pero no `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software`. `HKEY_LOCAL_MACHINE\system\ControlSet*` no es una ruta válida a una clave de registro. Una ruta a una clave de registro que contenga * define “esta ruta o cualquier ruta de cualquier nivel que se encuentre después de ese símbolo”. Esta es la única manera de usar caracteres globales para archivos de destino.

Primero se evaluará la parte específica de la ruta, y luego la ruta que sigue al carácter global (*).

ADVERTENCIA

Si crea una regla muy genérica, se mostrará la advertencia sobre este tipo de regla.

4.2.12.2 Configuración avanzada

Las opciones que se muestran a continuación resultan útiles para la depuración y el análisis de la conducta de una aplicación:

Controladores siempre permitidos para cargar: los controladores seleccionados siempre tienen permitido cargar independientemente del modo de filtrado configurado, a menos que se bloquee explícitamente por una regla de usuario.

Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se escribirán en el registro del sistema HIPS.

Notificar cuando ocurran cambios en las aplicaciones de inicio: muestra una notificación del escritorio cada vez que se agrega o quita una aplicación del inicio del sistema.

Consulte nuestro [Artículo de la base de conocimiento](#) para obtener una versión actualizada de esta página de ayuda.

4.2.12.2.1 Controladores siempre permitidos para cargar

Los controladores que se muestran en esta lista siempre tendrán permitido cargar independientemente del modo de filtrado de HIPS, a menos que se bloquee explícitamente por una regla de usuario.

Agregar: agrega un controlador nuevo.

Editar: edita la ruta para un controlador seleccionado.

Eliminar: elimina un controlador de la lista.

Restablecer: vuelve a cargar un conjunto de controladores del sistema.

NOTA

haga clic en **Restablecer** si no desea que se incluyan los controladores que ha agregado en forma manual. Esto puede ser útil si ha agregado varios controladores y no puede eliminarlos de la lista en forma manual.

4.3 Actualización

Las opciones de configuración de la actualización están disponibles en el árbol de **Configuración avanzada** (F5) en **Actualización > General**. Esta sección especifica la información del origen de la actualización, como los servidores de actualización que se usan y los datos de autenticación para estos servidores.

General

El perfil de actualización que actualmente está en uso se muestra en el menú desplegable **Perfil seleccionado**. Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**, ingrese su propio **Nombre de perfil**, y luego haga clic en **Agregar**.

En caso de que experimente problemas con una actualización, haga clic en **Borrar** para borrar el caché de actualización temporal.

Alertas de base de datos de firmas de virus obsoleta

Establecer automáticamente una edad máxima para la base de datos: permite establecer el tiempo máximo (en días) luego del cual se informará que la base de datos de firmas de virus está obsoleta. El valor predeterminado es 7.

Reversión

Si sospecha que la nueva actualización de la base de datos de virus o de los módulos de programas puede ser inestable o estar corrupta, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización

para un período elegido. O bien puede habilitar las actualizaciones que se deshabilitaron anteriormente si las pospuso de manera indefinida.

ESET Mail Security registra instantáneas de la base de datos de firmas de virus y de los módulos de programa para usar con la característica de *reversión*. Para crear instantáneas de la base de datos de virus, deje el interruptor **Crear instantáneas de los archivos de actualización** habilitado. El campo **Cantidad de instantáneas almacenadas localmente** define la cantidad de instantáneas anteriores de la base de datos de virus que se almacenaron.

Si hace clic en **Revertir (Configuración avanzada (F5) > Actualización > General)**, debe seleccionar un intervalo de tiempo del menú desplegable que represente el período en que se hará una pausa en las actualizaciones de la base de datos de firmas de virus y del módulo del programa.

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

GENERAL

Perfil seleccionado: Mi perfil

Lista de perfiles: Editar

Borrar caché de actualización: Borrar

ALERTAS DE BASE DE DATOS DE FIRMAS DE VIRUS OBSOLETA

Esta configuración define la antigüedad máxima permitida para la base de datos de firmas de virus antes de que se considere obsoleta, y una alerta se mostrará.

Establecer una antigüedad máxima para la base de datos automáticamente: ☒

Edad máxima para la base de datos (días): 7

REVERSIÓN

Crear instantáneas de archivos actualizados: ☒

Número de instantáneas almacenadas localmente: 2

Predeterminado Aceptar Cancelar

Para que las actualizaciones se descarguen correctamente, es esencial que complete correctamente todos los parámetros de actualización. Si usa un firewall, asegúrese de que el programa de ESET tenga permiso para comunicarse con Internet (por ejemplo, una comunicación HTTP).

De forma predeterminada, el **Tipo de actualización** (ubicado en **Básico**) está configurado en **Actualización normal** para garantizar que los archivos de actualización se descarguen automáticamente del servidor de ESET con la menor carga de tráfico de red.

Básico

Deshabilitar mostrar notificación acerca de actualización correcta: desactiva la notificación de la bandeja del sistema en el sector inferior derecho de la pantalla. Resulta útil seleccionar esta opción si se está ejecutando una aplicación de pantalla completa o un juego. Tenga en cuenta que el Modo presentación desactivará todas las notificaciones.

El menú **Servidor de actualización** está configurado en **SELECCIONAR AUTOMÁTICAMENTE** en forma predeterminada. El servidor de actualización es la ubicación donde se almacenan las actualizaciones. Si usa un servidor de ESET, recomendamos que deje seleccionada la opción predeterminada. Si estuvo usando un servidor de actualización personalizado y desea revertirlo al modo predeterminado, escriba **SELECCIONAR AUTOMÁTICAMENTE**. ESET Mail Security elegirá los servidores de actualización de ESET automáticamente.

Cuando use un servidor HTTP local (también conocido como Mirror), el servidor de actualización debe ingresarse de

la siguiente manera:

`http://computer_name_or_its_IP_address:2221`

Cuando use un servidor HTTP local con SSL, el servidor de actualización debe ingresarse de la siguiente manera:

`https://computer_name_or_its_IP_address:2221`

Cuando use una carpeta compartida local, el servidor de actualización debe configurarse de la siguiente manera:

`\\computer_name_or_its_IP_address\shared_folder`

Actualizar desde Mirror

La autenticación para los servidores de actualización está basada en la **Clave de licencia** generada y enviada al usuario después de la adquisición del producto. Al usar un servidor Mirror local, puede definir las credenciales para que los clientes se registren en el servidor Mirror antes de recibir las actualizaciones. En forma predeterminada, no se requiere ninguna verificación y los campos **Nombre de usuario** y **Contraseña** quedan vacíos.

4.3.1 Revertir actualización

Si hace clic en **Revertir (Configuración avanzada (F5) > Actualización > Perfil)**, debe seleccionar un intervalo de tiempo del menú desplegable que represente el período en que se hará una pausa en las actualizaciones de la base de datos de firmas de virus y del módulo del programa.

Seleccione **Hasta que se revoque** para posponer las actualizaciones regulares de manera indefinida hasta restaurar manualmente la funcionalidad de actualización. Debido a que esto representa un riesgo potencial para la seguridad, no recomendamos seleccionar esta opción.

La versión de la base de datos de firmas de virus regresa a la versión más antigua disponible y se guarda como una instantánea en el sistema local de archivos del equipo.

Ejemplo: Deje que el número 10646 sea la versión más reciente de la base de datos de firmas de virus. 10645 y 10643 se guardan como instantáneas de la base de datos de firmas de virus. Tenga en cuenta que 10644 no está disponible porque, por ejemplo, el equipo estaba apagado y se ofreció una actualización más reciente antes de descargar 10644. Si ha ingresado 2 en el campo **Cantidad de instantáneas almacenadas localmente** y hace clic en **Revertir**, la base de datos de firmas de virus (incluidos los módulos del programa) se restaurará a la versión número 10643. Este proceso puede tardar un poco. Revise si la versión de la base de datos de firmas de virus se ha revertido desde la ventana principal del programa de ESET Mail Security en la sección [Actualizar](#).

4.3.2 Modo de actualización

La pestaña **Modo de actualización** contiene las opciones relacionadas a la actualización de componentes del programa. El programa le permite al usuario predefinir su conducta cuando esté disponible un nuevo reemplazo de componentes del programa por una versión posterior.

Las actualizaciones de los componentes del programa incorporan nuevas características o incluyen modificaciones a las ya existentes en versiones anteriores. Puede realizarse automáticamente sin la intervención del usuario, pero también se puede elegir recibir una notificación. Luego de instalar la actualización de componentes del programa, es posible que se requiera reiniciar el equipo. En la sección **Actualización de componentes del programa** hay tres opciones disponibles:

- **Preguntar antes de descargar componentes del programa:** es la opción predeterminada. El programa le solicitará que confirme o rechace las actualizaciones de componentes del programa cuando estén disponibles.
- **Siempre actualizar los componentes del programa:** la actualización de componentes del programa se descargará e instalará automáticamente. Recuerde que puede llegar a ser necesario reiniciar el equipo.
- **Nunca actualizar los componentes del programa:** no se realizará ninguna actualización de componentes del programa en absoluto. Esta opción es adecuada para instalaciones en servidores, debido a que los servidores en general solo se pueden reiniciar durante su mantenimiento.

NOTA

la selección de la opción más apropiada depende de la estación de trabajo donde se aplicará la configuración. Tenga en cuenta que existen diferencias entre las estaciones de trabajo y los servidores; por ejemplo, el reinicio automático de un servidor después de la actualización de un programa podría provocar serios daños.

Si la opción **Preguntar antes de descargar la actualización** está activada, se mostrará una notificación cuando haya una nueva actualización disponible.

Si el tamaño del archivo de actualización es mayor que el valor especificado en el campo **Preguntar si un archivo de actualización es más grande que (kB)**, el programa mostrará una notificación.

4.3.3 Proxy HTTP

Si desea acceder a las opciones de configuración del servidor proxy para un perfil de actualización determinado, haga clic en **Actualización** en el árbol de **Configuración avanzada** (F5) y luego en **Proxy HTTP**. Haga clic en el menú desplegable **Modo de proxy** y seleccione una de las siguientes tres opciones:

- No usar servidor proxy
- Conexión a través de un servidor proxy
- Usar la configuración global del servidor proxy

Al seleccionar la opción **Usar la configuración global del servidor proxy**, se usarán las opciones de configuración del servidor proxy ya especificadas en la sección **Herramientas > Servidor proxy** del árbol de configuración avanzada.

Seleccione **No usar servidor proxy** para indicar que no se usará ningún servidor proxy para actualizar ESET Mail Security.

La opción **Conexión a través de un servidor proxy** debe estar seleccionada si:

- Debe usar un servidor proxy para actualizar ESET Mail Security, diferente del servidor proxy especificado en la configuración global (**Herramientas > Servidor proxy**). En ese caso, la configuración debe especificarse aquí: dirección del **Servidor proxy**, **Puerto** de comunicación (3128, en forma predeterminada), además del **Nombre de usuario** y la **Contraseña** para el servidor proxy, de ser necesario.
- La configuración del servidor proxy no se estableció en forma global, pero ESET Mail Security se conectará a un servidor proxy para descargar las actualizaciones.
- El equipo está conectado a Internet mediante un servidor proxy. Durante la instalación del programa, la configuración se copia de Internet Explorer, pero si posteriormente se cambia (por ej., cambia el ISP), verifique desde esta ventana que la configuración del proxy HTTP sea la correcta. De lo contrario, el programa no podrá conectarse a los servidores de actualización.

La configuración predeterminada para el servidor proxy es **Usar la configuración global del servidor proxy**.

NOTA

Los datos de autenticación como el **Nombre de usuario** y la **Contraseña** sirven para acceder al servidor proxy. Complete estos campos solo si el nombre de usuario y la contraseña son necesarios. Recuerde que estos campos no corresponden a su nombre de Usuario y Contraseña para ESET Mail Security y solo deben suministrarse si tiene la certeza de que se requiere una contraseña para acceder a Internet a través de un servidor proxy.

4.3.4 Conectarse a la LAN como

Cuando se lleva a cabo una actualización desde un servidor local con una versión del sistema operativo Windows NT, se requiere autenticar cada conexión de red en forma predeterminada.

Configuración avanzada

SEVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

+ GENERAL

Mi perfil

+ BÁSICO

+ MODO DE ACTUALIZACIÓN

+ PROXY HTTP

- CONECTARSE A LA LAN COMO

Tipo de usuario local

Cuenta del sistema (prede... ▼

Nombre de usuario

Contraseña

Desconectar del servidor tras la actualización

☐ x

+ REPLICACIÓN

Predeterminado

Aceptar

Cancelar

Para configurar dicha cuenta, seleccione en el menú desplegable **Tipo de usuario local**:

- **Cuenta del sistema (predeterminado)**
- **Usuario actual**
- **Usuario especificado**

Seleccione **Cuenta del sistema (predeterminado)** si desea usar la cuenta del sistema para la autenticación. Normalmente, no se lleva a cabo ningún proceso de autenticación si no se proporcionan los datos de autenticación en la sección principal correspondiente a la configuración de la actualización.

Para asegurar que el programa realice la autenticación mediante la cuenta de un usuario actualmente registrado, seleccione **Usuario actual**. La desventaja de esta solución es que el programa no podrá conectarse al servidor de actualización cuando no haya ningún usuario registrado.

Seleccione **Usuario especificado** si desea que el programa use la cuenta de un usuario específico para realizar la autenticación. Use este método cuando falle la conexión predeterminada de la cuenta del sistema. Recuerde que la cuenta de usuario especificada debe tener acceso al directorio de archivos de actualización en el servidor local. De lo contrario, el programa no podrá establecer una conexión y descargar las actualizaciones.

ADVERTENCIA

cuando esté seleccionado el **Usuario actual** o el **Usuario especificado**, puede aparecer un error al cambiar la identidad del programa según el usuario deseado. Es recomendable ingresar los datos de autenticación de la LAN en la sección principal correspondiente a la configuración de la actualización. En esta sección de configuración de la actualización, los datos de autenticación deben ingresarse de la siguiente forma: *nombre_de_dominio\usuario* (si es un grupo de trabajo, ingrese *nombre_del_grupo_de_trabajo\nombre*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no se necesita realizar ninguna autenticación.

Active **Desconectar del servidor después de la actualización** para forzar una desconexión si la conexión al servidor permanece activa aunque las actualizaciones se hayan terminado de descargar.

4.3.5 Mirror

ESET Mail Security le permite crear copias de archivos de actualización que se pueden usar para actualizar otras estaciones de trabajo en la red. El uso de un “*servidor reflejado*”: es conveniente tener una copia de los archivos de actualización en el entorno de la LAN debido a que las estaciones de trabajo no necesitan descargar los archivos de actualización desde el servidor de actualización del proveedor reiteradamente. Las actualizaciones se descargan al servidor reflejado local y, desde allí, se distribuyen a todas las estaciones de trabajo para evitar el riesgo de generar una sobrecarga en el tráfico de red. La actualización de las estaciones de trabajo del cliente desde un Mirror optimiza el equilibrio de carga de la red y preserva el ancho de banda de la conexión a Internet.

Las opciones de configuración del servidor Mirror local se encuentran en la Configuración avanzada en **Actualización**. Para acceder a esta sección, presione la tecla F5 para acceder a la Configuración avanzada, haga clic en **Actualizar** y seleccione la pestaña **Espejo**.

Para crear un servidor reflejado en la estación de trabajo del cliente, habilite **Crear mirror de actualización**. Al habilitar esta opción, se activan otras opciones de configuración del Mirror, tales como la forma de acceder a los archivos de actualización y la ruta de actualización a los archivos replicados.

Acceder a los archivos de actualización

- **Proporcionar archivos de actualización mediante el servidor HTTP interno:** si esta opción se encuentra habilitada, se puede acceder a los archivos de actualización a través de HTTP, sin necesidad de ingresar credenciales.

NOTA

Windows XP requiere service pack 2 o posteriores para usar el servidor HTTP.

Los métodos para acceder al servidor Mirror se describen en detalle en [Actualizar desde el Mirror](#). Existen dos métodos básicos para acceder al Mirror: la carpeta con los archivos de actualización puede presentarse como una

carpeta compartida de red, o los clientes pueden acceder al servidor reflejado ubicado en un servidor HTTP.

La carpeta destinada a almacenar los archivos de actualización para el Mirror se define en **Carpeta para almacenar los archivos replicados**. Haga clic en **Carpeta** para buscar una carpeta en el equipo local o una carpeta compartida en la red. Si la carpeta especificada requiere una autorización, deberá ingresar los datos de autenticación en los campos **Nombre de usuario** y **Contraseña**. Si la carpeta de destino seleccionada está en un disco de la red cuyo sistema operativo es Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada. El nombre de usuario y la contraseña se deben ingresar con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. Recuerde que debe proporcionar las contraseñas correspondientes.

- **Archivos:** al configurar el Mirror, también puede especificar las versiones de idiomas de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor reflejado configurado por el usuario.

Servidor HTTP

- **Puerto del servidor:** en forma predeterminada, el puerto del servidor está configurado en 2221.
- **Autenticación:** define el método de autenticación usado para acceder a los archivos de actualización. Se encuentran disponibles las siguientes opciones: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para usar la codificación de Base64 con la autenticación básica del nombre de usuario y la contraseña. La opción **NTLM** proporciona una codificación obtenida mediante un método seguro. Para la autenticación, se usa el usuario creado en la estación de trabajo que comparte los archivos de actualización. La configuración predeterminada es **NINGUNA**, que otorga acceso a los archivos de actualización sin necesidad de autenticar.

Añada su **Archivo de cadena de certificados** o genere un certificado de firma automática si desea ejecutar el servidor HTTP con el soporte de HTTPS (SSL). Se encuentran disponibles los siguientes tipos de certificado: ASN, PEM y PFX. Para obtener una seguridad adicional, puede usar el protocolo HTTPS para descargar los archivos de actualización. Es casi imposible realizar un seguimiento de las transferencias de datos y credenciales de registro con este protocolo. La opción **Tipo de clave privada** está configurada en **Integrada** de forma predeterminada (y por lo tanto, la opción **Archivo de clave privada** está deshabilitada de forma predeterminada). Esto significa que la clave privada es parte del archivo de cadena de certificados seleccionado.

Conectarse a la LAN como

- **Tipo de usuario local:** las configuraciones **Cuenta del sistema (predeterminada)**, **Usuario actual**, y **Usuario especificado** se mostrarán en los menús desplegables correspondientes. Las configuraciones de **Nombre de usuario** y **Contraseña** son opcionales. Consulte [Conectarse a la LAN como](#).
- Seleccione **Desconectar del servidor tras la actualización** para forzar una desconexión si la conexión al servidor permanece activa después de que las actualizaciones se hayan terminado de descargar.

Actualización de componentes del programa

- **Actualizar componentes automáticamente:** permite la instalación de nuevas funciones y las actualizaciones de las funciones existentes. Puede realizarse una actualización automáticamente sin la intervención del usuario, pero también se puede elegir recibir una notificación. Luego de instalar la actualización de componentes del programa, es posible que se requiera reiniciar el equipo.
- **Actualizar componentes ahora:** actualiza los componentes de su programa a la versión más reciente.

4.3.5.1 Actualización desde el mirror

Existen dos métodos básicos para configurar un Mirror, que es esencialmente un repositorio desde donde los clientes pueden descargar archivos de actualización. La carpeta con los archivos de actualización se puede presentar como una carpeta compartida de red o como un servidor HTTP.

Acceso al Mirror mediante un servidor HTTP interno

Esta es la configuración predeterminada, que se especifica en la configuración predefinida del programa. Para permitir el acceso al Mirror mediante el servidor HTTP, vaya a **Configuración avanzada > Actualización > Mirror**, y seleccione **Crear servidor reflejado de actualización**.

En la sección **Servidor HTTP** de la pestaña **Mirror**, puede especificar el **Puerto del servidor** donde escuchará el servidor HTTP, así como el tipo de **Autenticación** que usa el servidor HTTP. En forma predeterminada, el puerto del servidor está establecido en **2221**. La opción **Autenticación** define el método de autenticación usado para acceder a los archivos de actualización. Se encuentran disponibles las siguientes opciones: **Ninguna**, **Básica** y **NTLM**.

- Seleccione **Básica** para usar la codificación de Base64 con la autenticación básica del nombre de usuario y la contraseña.
- La opción **NTLM** proporciona una codificación obtenida mediante un método seguro. Para la autenticación, se usa el usuario creado en la estación de trabajo que comparte los archivos de actualización.
- La configuración predeterminada es **Ninguna**, que otorga acceso a los archivos de actualización sin necesidad de autenticar.

ADVERTENCIA

Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta del Mirror debe estar ubicada en el mismo equipo que la instancia de ESET Mail Security que la crea.

SSL para el servidor HTTP

Añada su **Archivo de cadena de certificados** o genere un certificado de firma automática si desea ejecutar el servidor HTTP con el soporte de HTTPS (SSL). Se encuentran disponibles los siguientes tipos de certificado: **PEM**, **PFX** y **ASN**. Para obtener una seguridad adicional, puede usar el protocolo HTTPS para descargar los archivos de actualización. Es casi imposible realizar un seguimiento de las transferencias de datos y credenciales de registro con este protocolo. El **Tipo de clave privada** está configurado en **Integrada** en forma predeterminada, lo que significa que la clave privada es un componente del archivo de cadena de certificados seleccionado.

NOTA

El error **Nombre de usuario y/o contraseña no válidos** aparecerá en el panel de actualización del menú principal luego de varios intentos fallidos de actualizar la base de datos de firmas de virus del Mirror. Recomendamos que vaya a **Configuración avanzada > Actualización > Mirror**, y verifique el Nombre de usuario y la Contraseña. El motivo más común de este error es el ingreso incorrecto de los datos de autenticación.

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO

HERRAMIENTAS

INTERFAZ DEL USUARIO

ARCHIVOS

Archivos

Editar

SEVIDOR HTTP

Puerto de servidor

2221

Autenticación

Ninguno

SSL PARA EL SERVIDOR HTTP

Archivo de cadena de certificados

...

Tipo de certificado

PEM

Archivo de clave privada

...

Tipo de clave privada

Integrados

CONECTARSE A LA LAN COMO

ACTUALIZACIÓN DE COMPONENTES DEL PROGRAMA

Predeterminado

Aceptar

Cancelar

Después de configurar su servidor Mirror, debe agregar el nuevo servidor de actualización en las estaciones de trabajo del cliente. Para hacerlo, siga estos pasos:

- Acceda a la **Configuración avanzada** (F5) y haga clic en **Actualización > Básico**.
- Quite **Elegir automáticamente** y agregue un nuevo servidor al **campo** Servidor de actualización mediante uno de los siguientes formatos:
http://IP_address_of_your_server:2221
https://IP_address_of_your_server:2221 (si se usa SSL)

Acceder al Mirror mediante el uso compartido del sistema

En primer lugar, se debe crear una carpeta compartida en un dispositivo local o de red. Cuando se crea la carpeta para el Mirror, se deberá proporcionar el acceso de *“escritura”* para el usuario que guardará los archivos de actualización en la carpeta y el acceso de *“lectura”* para todos los usuarios que actualizarán ESET Mail Security desde la carpeta del Mirror.

A continuación, configure el acceso al Mirror en **Configuración avanzada > Actualización** pestaña **Mirror** al deshabilitar la opción **Proporcionar archivos de actualización mediante el servidor HTTP interno**. Esta opción está habilitada en forma predeterminada en el paquete de instalación del programa.

Si la carpeta compartida se ubica en otro equipo de la red, es necesario ingresar los datos de autenticación para acceder al otro equipo. Para ingresar los datos de autenticación, abra ESET Mail Security, **Configuración avanzada** (F5) y haga clic en **Actualización > Conectarse a la LAN como**. Esta configuración es la misma que se usa para la actualización, como se describe en la sección [Conectarse a la LAN como](#).

Cuando la configuración del Mirror (Espejo) esté completa, en las estaciones de trabajo del cliente establezca `\\UNC\ RUTA` como el servidor de actualización, siguiendo los pasos que figuran a continuación:

1. Abra ESET Mail Security **Configuración avanzada** y haga clic en **Actualización > Básico**.
2. Haga clic en **Servidor de actualización** y agregue un nuevo servidor con el formato `\\UNC\ RUTA`.

i NOTA

Para un funcionamiento correcto de las actualizaciones, deberá especificar la ruta a la carpeta del Mirror como una ruta UNC. Es posible que no funcionen las actualizaciones de las unidades asignadas.

La última sección controla los componentes del programa (PCU). De forma predeterminada, los componentes del programa descargados están preparados para copiarse en el servidor reflejado local. Si se activa **Actualizar los componentes del programa**, no es necesario hacer clic en **Actualización**, ya que los archivos se copian en el servidor reflejado local automáticamente cuando están disponibles. Consulte el [Modo de actualización](#) para obtener más información sobre las actualizaciones del componente del programa.

4.3.5.2 Archivos espejo

Lista de los archivos disponibles y localizados de los componentes del programa.

4.3.5.3 Resolución de problemas de actualización desde el mirror

En la mayoría de los casos, los problemas durante una actualización desde un servidor Mirror son causados por una o más de las siguientes: especificación incorrecta de las opciones de la carpeta del Mirror, datos de autenticación incorrectos para acceder a la carpeta del Mirror, configuración incorrecta en las estaciones de trabajo locales que intentan descargar archivos de actualización desde el Mirror, o una combinación de las razones mencionadas. A continuación, se muestra información general sobre los problemas más frecuentes que pueden surgir durante una actualización desde el mirror:

- **ESET Mail Security informa que se produjo un error al conectarse con el servidor Mirror:** probablemente causado por la especificación incorrecta del servidor de actualización (la ruta de red a la carpeta del Mirror) desde donde las estaciones de trabajo locales descargan las actualizaciones. Para verificar la carpeta, haga clic en el menú **Inicio** de Windows, haga clic en **Ejecutar**, ingrese el nombre de la carpeta y haga clic en **Aceptar**. Se debe mostrar el contenido de la carpeta.
- **ESET Mail Security requiere un nombre de usuario y una contraseña:** probablemente causado por datos de autenticación incorrectos (nombre de usuario y contraseña) en la sección de actualización. Se usan el nombre de usuario y la contraseña para otorgar acceso al servidor de actualización, desde donde el programa se actualizará. Asegúrese que la información de autenticación sea correcta y se haya ingresado en el formato correcto. Por ejemplo, *Dominio/Nombre de usuario* o *Grupo de trabajo/Nombre de usuario*, con sus contraseñas correspondientes. Si cualquier persona puede acceder al servidor Mirror, esté al tanto que esto no significa que cualquier usuario tiene acceso. “Cualquier persona” no significa cualquier usuario no autorizado, sólo significa que todos los usuarios del dominio pueden acceder a la carpeta. Como resultado, si “Cualquier persona” puede acceder a la carpeta, el nombre de usuario y la contraseña del dominio deberá ingresarse en la sección de configuración de la actualización.
- **ESET Mail Security informa que se produjo un error al conectarse con el servidor Mirror:** la comunicación en el puerto definido para acceder a la versión HTTP del Mirror está bloqueada.

4.3.6 Cómo crear tareas de actualización

Las actualizaciones pueden accionarse manualmente con un clic en **Actualizar la base de datos de firmas de virus** en la ventana primaria que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también pueden ejecutarse como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas > Tareas programadas**. Las siguientes tareas se encuentran activas en forma predeterminada en ESET Mail Security:

- **Actualización automática de rutina**
- **Actualización automática después de la conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**

Cada tarea de actualización puede modificarse acorde a sus necesidades. Además de las tareas de actualización predeterminadas, puede crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más detalles sobre la creación y la configuración de tareas de actualización, consulte la sección [Tareas programadas](#) de esta guía.

4.4 Internet y correo electrónico

La sección **Internet y correo electrónico** permite configurar la [Protección del cliente de correo electrónico](#), proteger la comunicación por Internet mediante la [Protección del acceso a la Web](#) y controlar los protocolos de Internet con la configuración del [Filtrado de protocolos](#). Estas características son vitales para proteger el equipo mientras se comunica por Internet.

La **Protección del cliente de correo electrónico** controla toda la comunicación por correo electrónico, protege ante códigos maliciosos y permite elegir la acción a realizar cuando se detecta una infección.

Protección del acceso a la Web: monitorea la comunicación entre los navegadores web y los servidores remotos, según las disposiciones normativas de HTTP y HTTPS. Esta característica también permite bloquear, permitir o excluir ciertas [Direcciones URL](#).

El **Filtrado de protocolos** es una protección avanzada para los protocolos de aplicación, provista por el motor de exploración ThreatSense. Este control funciona automáticamente, más allá de que se use un navegador web o un cliente de correo electrónico. También funciona para las comunicaciones encriptadas ([SSL/TLS](#)).

i NOTA

En Windows Server 2008 y Windows Server 2008 R2, la instalación del componente **Internet y correo electrónico** está desactivada de manera predeterminada. Si desea instalar esta función, seleccione el [tipo de instalación Personalizada](#). Si ESET Mail Security ya está instalado, puede volver a ejecutar el instalador nuevamente para modificar la instalación existente agregando el componente de Internet y correo electrónico.

4.4.1 Filtrado de protocolos

El motor de exploración ThreatSense, que integra perfectamente todas las técnicas avanzadas para la exploración de malware, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona en forma automática, independientemente del navegador de Internet o del cliente de correo electrónico usado. Para editar ajustes encriptados (SSL), ingrese en **Internet y correo electrónico > SSL/TLS**.

Habilitar el filtrado del contenido de los protocolos de aplicación: se puede usar para deshabilitar el filtrado de protocolos. Tenga en cuenta que muchos de los componentes de ESET Mail Security (Protección del acceso a la web, Protección de los protocolos de correo electrónico y Antiphishing) dependen de esto y no funcionarán sin él.

Aplicaciones excluidas: le permite excluir del filtrado de protocolos direcciones remotas específicas. Es útil cuando el filtrado de protocolos causa problemas de compatibilidad.

Direcciones IP excluidas: le permite excluir del filtrado de protocolos aplicaciones específicas. Es útil cuando el filtrado de protocolos causa problemas de compatibilidad.

Clientes de Internet y correo electrónico: solo se usa en los sistemas operativos de Windows, y le permite

seleccionar las aplicaciones para las que se filtra todo el tráfico mediante el filtrado de protocolos, independientemente de los puertos usados.

4.4.1.1 Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones específicas con reconocimiento de redes, selecciónelas de la lista. La comunicación HTTP/POP3 de las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable usar esta opción solo para aplicaciones que no funcionen correctamente cuando se verifica su comunicación.

Las aplicaciones y los servicios que ya fueron afectados por el filtrado de protocolos se mostrarán automáticamente después de hacer clic en **Agregar**.

Editar: edite las entradas seleccionadas de la lista.

Quitar: elimine las entradas seleccionadas de la lista.

4.4.1.2 Direcciones IP excluidas

Las direcciones IP en esta lista se excluirán del filtrado de contenido del protocolo. La comunicación HTTP/POP3/IMAP desde o hacia las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable que únicamente use esta opción para las direcciones confiables conocidas.

Agregar: haga clic para agregar una dirección IP, un rango de direcciones o una subred de un punto remoto, al que se debe aplicar la regla.

Editar: edite las entradas seleccionadas de la lista.

Quitar: elimine las entradas seleccionadas de la lista.

4.4.1.3 Clientes de Internet y correo electrónico

Dada la enorme cantidad de códigos maliciosos que circulan por Internet, la navegación segura es un aspecto crucial para la protección de los equipos. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código malicioso para introducirse en el sistema de incógnito; por este motivo, ESET Mail Security se centra en la seguridad de los navegadores web. Todas las aplicaciones que accedan a la red se pueden marcar como navegadores de internet. Las aplicaciones que ya usan los protocolos para la comunicación o las aplicaciones desde la ruta seleccionada se pueden agregar en la lista de clientes de Internet y correo electrónico.

NOTA

desde Windows Vista Service Pack 1 y Windows Server 2008, la nueva arquitectura de la Plataforma de filtrado de Windows (WFP) se usa para verificar la comunicación de red. La tecnología WFP usa técnicas de monitoreo especiales, por lo que la sección **Clientes de Internet y correo electrónico** no está disponible.

4.4.2 SSL/TLS

ESET Mail Security tiene la capacidad de verificar las amenazas en las comunicaciones que usan el protocolo SSL/TLS. Puede usar varios modos de exploración para examinar las comunicaciones protegidas por SSL mediante certificados de confianza, certificados desconocidos o certificados excluidos de la verificación de las comunicaciones protegidas por SSL.

Habilitar el filtrado de protocolos SSL/TLS: si se deshabilita el filtrado de protocolos, el programa no explorará las comunicaciones con el protocolo SSL/TLS.

El modo de filtrado de protocolos SSL/TLS está disponible en las siguientes opciones:

- **Modo automático:** seleccione esta opción para explorar todas las comunicaciones protegidas por SSL/TLS excepto las protegidas por certificados excluidos de la verificación. Si se establece una nueva comunicación que use un certificado firmado desconocido, no se notificará al usuario y se filtrará la comunicación en forma automática. Al acceder a un servidor con un certificado no confiable que está marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.
- **Modo interactivo:** si ingresa un nuevo sitio protegido por SSL/TLS (con un certificado desconocido), se mostrará un

cuadro de diálogo para la selección de la acción. Este modo le permite crear una lista de certificados SSL/TLS que se excluirán de la exploración.

Bloquear las comunicaciones cifradas usando el protocolo obsoleto SSL v2: las comunicaciones que usen la versión anterior del protocolo SSL serán automáticamente bloqueadas.

Certificado raíz

Certificado raíz: para que la comunicación SSL/TLS funcione correctamente en los navegadores o clientes de correo electrónico, es imprescindible agregar el certificado raíz para ESET a la lista de certificados raíz conocidos (desarrolladores). **Agregar el certificado raíz a los navegadores conocidos** deberá estar habilitada. Seleccione esta opción para agregar automáticamente el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no compatibles, haga clic en **Ver el certificado > Detalles > Copiar en el archivo...** y luego impórtelo manualmente al navegador.

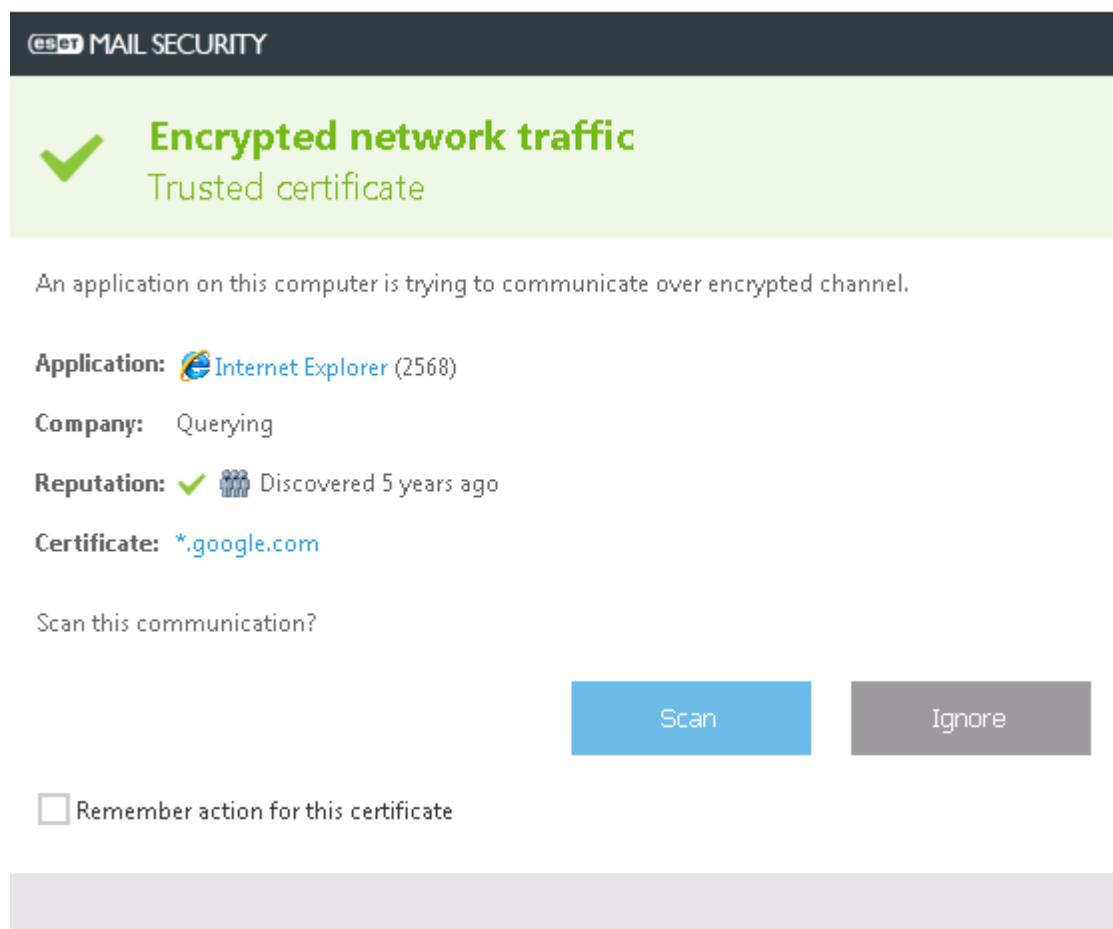
Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificados de TRCA: en algunos casos, el certificado de un sitio web no se puede verificar mediante el almacén de Entidades de certificación de raíz de confianza (TRCA). Esto significa que alguien firma automáticamente el certificado (por ejemplo, el administrador de un servidor web o una pequeña empresa); por lo que considerar este certificado como confiable no siempre es un riesgo. La mayoría de los negocios (por ejemplo, los bancos) usan un certificado firmado por las TRCA. Si se selecciona **Preguntar sobre la validez del certificado** (predeterminado), el programa le indicará al usuario que seleccione la acción a realizar cuando se establezca una comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a los sitios con certificados no verificados.

Si el certificado no es válido o está dañado: esto significa que el certificado está vencido o no fue firmado correctamente. En este caso, es recomendable que deje **Bloquear las comunicaciones que usan el certificado** seleccionado.

La **Lista de certificados conocidos** le permite personalizar la conducta de ESET Mail Security para certificados SSL específicos.

4.4.2.1 Comunicación cifrada SSL



Si su sistema está configurado para usar una exploración del protocolo SSL, se mostrará una ventana de diálogo para elegir una acción en dos situaciones distintas:

Primero, si un sitio web usa un certificado no válido o que no se puede verificar, y ESET Mail Security está configurado para preguntarle al usuario en dichos casos (de forma predeterminada, sí para los certificados que no se pueden verificar; no para los que no son válidos), un cuadro de diálogo le preguntará si desea **Permitir** o **Bloquear** la conexión.

Segundo, si el **modo de filtrado de protocolos SSL** está configurado en **Modo interactivo**, un cuadro de diálogo para cada sitio web le preguntará si desea **Explorar** o **Ignorar** el tráfico. Algunas aplicaciones verifican que su tráfico SSL no esté modificado ni inspeccionado por nadie; en dichos casos, ESET Mail Security debe **Ignorar** dicho tráfico para que la aplicación siga funcionando.

En los dos casos, el usuario puede elegir recordar la acción seleccionada. Las acciones guardadas se almacenan en la **Lista de certificados conocidos**.

4.4.2.2 Lista de certificados conocidos

Puede usar la lista de certificados conocidos para personalizar la conducta de ESET Mail Security para certificados SSL específicos y para recordar las acciones elegidas si selecciona el modo Interactivo en el modo de filtrado de protocolos SSL. La lista se puede ver y editar en **Configuración avanzada (F5) > Internet y correo electrónico > Verificación del protocolo SSL > Lista de certificados conocidos**.

La ventana **Lista de certificados conocidos** consta de:

Columnas

- **Nombre:** nombre del certificado.
- **Emisor del certificado:** nombre del creador del certificado.
- **Sujeto del certificado:** el campo del sujeto identifica la entidad asociada con la clave pública almacenada en el campo de la clave pública del sujeto.
- **Acceso :** seleccione **Permitir** o **Bloquear** como la **Acción de acceso** para permitir o bloquear la comunicación asegurada por este certificado, independientemente de su confianza. Seleccione **Auto** para permitir certificados de confianza y solicitar los que no son de confianza. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.
- **Explorar :** seleccione **Explorar** o **Ignorar** como la **Acción de exploración** para explorar o ignorar la comunicación asegurada por este certificado. Seleccione **Auto** para explorar en el modo automático y preguntar en el modo interactivo. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Elementos de control

- **Editar:** seleccione el certificado que desea configurar y haga clic en **Editar**.
- **Quitar:** seleccione el certificado que desea eliminar y haga clic en **Quitar**.
- **Aceptar/cancelar:** haga clic en **Aceptar** si desea guardar los cambios o en **Cancelar** si desea salir sin guardar.

4.4.3 Protección del cliente de correo electrónico

La integración de ESET Mail Security con los clientes de correo electrónico incrementa el nivel de protección activa frente a códigos maliciosos en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, esta integración se puede habilitar en ESET Mail Security. Cuando se activa la integración, la barra de herramientas de ESET Mail Security se inserta directamente en el cliente de correo electrónico (la barra de herramientas para las versiones más recientes de Windows Live Mail no se inserta), lo que permite una protección de correo electrónico más eficaz. Las configuraciones de la integración se ubican en **Configuración > Configuración avanzada > Internet y correo electrónico > Protección del cliente de correo electrónico > Clientes de correo electrónico**.

Integración con el cliente de correo electrónico

Entre los clientes de correo electrónico actualmente compatibles, se incluyen Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La ventaja principal de este complemento es su independencia respecto al protocolo usado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus. Si desea obtener una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de la Base de conocimiento de ESET](#).

Incluso si la integración no está habilitada, la comunicación por correo electrónico está protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

Active **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si nota que el sistema funciona con mayor lentitud mientras trabaja con su cliente de correo electrónico (solo MS Outlook). Esto puede ocurrir cuando se recupera el correo electrónico desde Kerio Outlook Connector Store.

Correo electrónico para explorar

Correo electrónico recibido: activa o desactiva la verificación de los mensajes recibidos.

Correo electrónico enviado: activa o desactiva la verificación de los mensajes enviados.

Correo electrónico leído: activa o desactiva la verificación de los mensajes leídos.

Acción para realizar en los correos electrónicos infectados

Sin acción: si se habilita esta opción, el programa identificará los archivos adjuntos infectados, pero dejará intactos los correos electrónicos, sin realizar acción alguna.

Eliminar correo electrónico: el programa notificará al usuario sobre las infiltraciones y eliminará el mensaje.

Mover el correo electrónico a la carpeta de elementos eliminados: los correos electrónicos infectados se enviarán automáticamente a la carpeta de elementos eliminados.

Mover el correo electrónico a la carpeta: los correos electrónicos infectados se enviarán automáticamente a la carpeta especificada.

Carpeta: especificar la carpeta personalizada donde desea mover los correos electrónicos infectados al detectarlos.

Repetir la exploración tras la actualización: activa o desactiva la exploración reiterada luego de actualizar la base de datos de firmas de virus.

Aceptar los resultados de las exploraciones realizadas por otros módulos: si se selecciona, el módulo de protección de correo electrónico aceptará los resultados de la exploración de otros módulos de protección (POP3, exploración de protocolos IMAP).

4.4.3.1 Protocolos de correo electrónico

Los protocolos IMAP y POP3 son de uso más generalizado y reciben comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. ESET Mail Security proporciona protección para estos protocolos, independientemente del cliente de correo electrónico que use y sin requerir una nueva configuración del cliente de correo electrónico.

Puede configurar la verificación de los protocolos IMAP/IMAPS y POP3/POP3S en la Configuración avanzada. Para acceder a esta configuración, expanda **Internet y correo electrónico > Protección del cliente de correo electrónico > Protocolos de correo electrónico**.

ESET Mail Security también admite la exploración de los protocolos IMAPS y POP3S, que usan un canal cifrado para transferir información entre el servidor y el cliente. ESET Mail Security verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en los puertos usados por los protocolos IMAPS/POP3S, independientemente de la versión del sistema operativo.

Las comunicaciones cifradas no se explorarán cuando se usen las configuraciones predeterminadas. Para habilitar la exploración de la comunicación cifrada, navegue a [Verificación de protocolos SSL/TLS](#) dentro de Configuración avanzada, haga clic en **Internet y correo electrónico > SSL/TLS** y seleccione **Habilitar filtrado de protocolos SSL/TLS**.

4.4.3.2 Alertas y notificaciones

La protección del correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Mediante el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Mail Security proporciona el control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Al examinar los mensajes entrantes, el programa usa todos los métodos avanzados de exploración incluidos en el motor de exploración ThreatSense. Esto significa que la detección de programas maliciosos se lleva a cabo incluso antes de verificar su coincidencia con la base de datos de firmas de virus. La exploración de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico usado.

Las opciones para esta funcionalidad están disponibles en **Configuración avanzada** bajo **Internet y correo electrónico > Protección del cliente de correo electrónico > Alertas y notificaciones**.

ThreatSense parámetros: la configuración avanzada del módulo de exploración de virus le permite configurar los objetos para explorar, los métodos de detección, etc. Haga clic para visualizar la ventana de configuración detallada

del módulo de exploración de virus.

Luego de verificar el correo electrónico, se puede añadir al mensaje una notificación con el resultado de la exploración. Puede elegir **Añadir mensajes de etiqueta a los correos electrónicos recibidos y leídos**, **Añadir una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos** o **Añadir mensajes de etiqueta a los correos electrónicos enviados**. Tenga en cuenta que, en ocasiones raras, los mensajes de etiqueta pueden ser omitidos en mensajes HTML problemáticos o si los mensajes están adulterados por malware. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías. Las opciones disponibles son:

- **Nunca:** no se agregará ningún mensaje de etiqueta en absoluto.
- **Solo al correo electrónico infectado:** únicamente se marcarán como verificados los mensajes que contengan software malicioso (predeterminado).
- **A todos los correos electrónicos explorados:** el programa añadirá mensajes a todos los correos electrónicos explorados.

Añadir una nota al asunto de los correos electrónicos infectados que fueron enviados: deshabilite esto si no desea que la protección de correo electrónico incluya una advertencia sobre virus en el asunto de un correo electrónico infectado. Esta característica hace posible realizar un filtrado simple del correo electrónico basado en el asunto (si es compatible con el programa de correo electrónico). También incrementa el nivel de credibilidad para el destinatario y si se detecta una amenaza, proporciona información valiosa sobre el grado de peligro de la amenaza de un correo electrónico o remitente específicos.

Plantilla añadida al asunto del correo electrónico infectado: si desea modificar el formato del prefijo en el asunto de un correo electrónico infectado, edite esta plantilla. Esta función reemplazará el asunto del mensaje “*Hola*” con un valor de prefijo dado “[virus]” por el siguiente formato: “[virus] *Hola*”. La variable %VIRUSNAME% representa la amenaza detectada.

4.4.3.3 Barra de herramientas de MS Outlook

El módulo de protección de Microsoft Outlook funciona como un complemento. Tras instalar ESET Mail Security, se agrega a Microsoft Outlook la siguiente barra de herramientas con las opciones de protección antivirus:

ESET Mail Security: al hacer clic en el ícono, se abre la ventana principal del programa de ESET Mail Security.

Volver a explorar los mensajes: permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte la sección [Protección del cliente de correo electrónico](#).

Configuración del módulo de exploración: muestra las opciones de configuración de la [Protección del cliente de correo electrónico](#).

4.4.3.4 Barra de herramientas de Outlook Express y Windows Mail

El módulo de protección de Outlook Express y Windows Mail funciona como un complemento. Tras instalar ESET Mail Security, se agrega a Outlook Express o a Windows Mail la siguiente barra de herramientas con las opciones de protección antivirus:

ESET Mail Security: al hacer clic en el ícono, se abre la ventana principal del programa de ESET Mail Security.

Volver a explorar los mensajes: permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte la sección [Protección del cliente de correo electrónico](#).

Configuración del módulo de exploración: muestra las opciones de configuración de la [Protección del cliente de correo electrónico](#).

Interfaz del usuario

Personalizar la apariencia: se puede modificar el aspecto de la barra de herramientas según el cliente de correo electrónico. Anule la selección de la opción para personalizar el aspecto de manera independiente a los parámetros del programa de correo electrónico.

Mostrar el texto: ver las descripciones de los íconos.

Texto a la derecha: las descripciones de las opciones se mueven del sector inferior al lado derecho de los íconos.

Íconos grandes: muestra íconos grandes para las opciones del menú.

4.4.3.5 Cuadro de diálogo de confirmación

Esta notificación sirve para corroborar que el usuario realmente desea realizar la acción seleccionada para eliminar, de esta forma, posibles errores. Por otro lado, el cuadro de diálogo también ofrece la opción de deshabilitar las confirmaciones.

4.4.3.6 Exploración reiterada de los mensajes

La barra de herramientas de ESET Mail Security, integrada en los clientes de correo electrónico, les permite a los usuarios especificar varias opciones de verificación del correo electrónico. La opción **Volver a explorar los mensajes** ofrece dos modos de exploración:

Todos los mensajes de la carpeta actual: explora los mensajes en la carpeta actualmente abierta.

Solo los mensajes seleccionados: explora únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a explorar los mensajes ya explorados** le proporciona al usuario la opción de realizar otra exploración en los mensajes que ya se habían explorado antes.

4.4.4 Protección del acceso a la Web

La conectividad a Internet es una característica estándar en la mayoría de los equipos personales. Lamentablemente, también se convirtió en el medio principal para transferir códigos maliciosos. La función de la protección del acceso web es monitorear la comunicación entre los navegadores web y los servidores remotos, según las disposiciones normativas de HTTP (protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se conocen por contenido malicioso se bloquea antes de que se descargue el contenido. Las demás páginas usan son exploradas por el motor de exploración ThreatSense cuando se cargan, y se bloquean si se detecta contenido malicioso. La protección del acceso web ofrece dos niveles de protección: bloqueo según la lista negra y bloqueo según el contenido.

Se recomienda firmemente que deje la protección del acceso web habilitada. Puede acceder a esta opción desde la ventana principal del programa de ESET Mail Security; para ello, vaya a **Configuración > Equipo > Protección del acceso a la Web**.

Las siguientes opciones están disponibles en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del acceso a la Web**:

- **Básico:** le permite habilitar o deshabilitar la protección del acceso a la Web en su totalidad. Si está deshabilitado, las siguientes opciones se desactivarán.
- **Protocolos web :** le permite configurar la supervisión de estos protocolos estándar, que son usados por la mayoría de los navegadores de Internet.

En forma predeterminada, ESET Mail Security está configurado para supervisar el protocolo HTTP que se usa en la mayoría de los navegadores de Internet.

NOTA

En Windows Vista y posteriores, el tráfico de HTTP siempre se supervisa en todos los puertos para todas las aplicaciones. En Windows XP/2003, puede modificar los Puertos usados por el protocolo HTTP en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del acceso a la Web > Protocolos web > Configuración de la exploración de HTTP**. El tráfico de HTTP se supervisa en los puertos especificados para todas las aplicaciones y en todos los puertos para las aplicaciones marcadas como Clientes de Internet y correo electrónico.

ESET Mail Security también admite la verificación del protocolo HTTPS. La comunicación de HTTPS usa un canal cifrado para transferir información entre el servidor y el cliente. ESET Mail Security verifica la comunicación

mediante los protocolos SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en Puertos usados por los protocolos HTTP, independientemente de la versión del sistema operativo.

La comunicación cifrada no se explorará cuando se usen las configuraciones predeterminadas. Para habilitar la exploración de la comunicación cifrada, navegue a [Verificación del protocolo SSL](#) en la Configuración avanzada, haga clic en **Internet y correo electrónico > Verificación del protocolo SSL** y seleccione **Habilitar filtrado de protocolos SSL**.

- [Administración de direcciones URL](#) : le permite especificar las direcciones HTTP que se desean bloquear, permitir o excluir de la verificación.
- [Configuración de los parámetros del motor ThreatSense](#): la configuración avanzada del módulo de exploración de virus le permite configurar propiedades, como los tipos de objetos que se explorarán (correos electrónicos, archivos comprimidos, etc.), los métodos de detección para la protección del acceso a la Web, etc.

4.4.4.1 Básico

Elija si desea que la opción **Protección del acceso a la Web** esté habilitada (predeterminado) o deshabilitada. Si está deshabilitado, las siguientes opciones se desactivarán.

NOTA

Se recomienda firmemente que deje la protección del acceso web habilitada. Puede acceder a esta opción desde la ventana principal del programa de principal de ESET Mail Security cuando vaya a **Configuración > Equipo > Protección del acceso a la Web**.

4.4.4.2 Administración de direcciones URL

La sección sobre la administración de direcciones URL le permite especificar las direcciones HTTP que se desean bloquear, permitir o excluir de la verificación.

No será posible acceder a los sitios web incluidos en la lista de direcciones bloqueadas, a menos que también estén incluidos en la lista de direcciones permitidas. Los sitios web en la lista de direcciones excluidas de la verificación no se exploran en busca de códigos maliciosos cuando se accede a los mismos.

[Habilitar el filtrado de protocolos SSL/TLS](#) debe estar seleccionado si desea filtrar las direcciones HTTPS además de las páginas Web HTTP. De lo contrario, solo se agregarán los dominios de los sitios HTTPS que haya visitado, y no se agregará la URL completa.

En todas las listas, pueden usarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco representa cualquier número o carácter, mientras que el signo de interrogación representa cualquier carácter. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se usan correctamente en esta lista.

Si desea bloquear todas las direcciones HTTP excepto las direcciones presentes en la **Lista de direcciones permitidas** activa, agregue un * a la **Lista de direcciones bloqueadas** activa.

Agregar: crea una lista nueva, además de las predefinidas. Esto puede ser útil si desea separar de manera lógica los diferentes grupos de direcciones. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que una segunda lista puede contener su propia lista negra, lo que facilitaría la actualización de la lista externa y mantendría intacta la suya.

Editar: modifica las listas existentes. Use esto para agregar o eliminar las direcciones de las listas.

Quitar: elimina las listas existentes. Solo es posible para las listas creadas con la opción Agregar, no con las opciones predeterminadas.

4.4.4.2.1 Creación de una nueva lista

Esta sección le permitirá indicar las listas de direcciones/máscaras URL que se bloquearán, permitirán o excluirán de la verificación.

Al crear una lista nueva, las siguientes opciones de configuración se encuentran disponibles:

Tipo de lista de direcciones: hay tres tipos de listas disponibles:

- **Lista de direcciones excluidas de la verificación:** no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones permitidas:** si se habilita **Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas**, y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones que se encuentran en esta lista. Las direcciones de esta lista se permiten incluso si están incluidas en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas :** el usuario no tendrá acceso a las direcciones especificadas en esta lista, a menos que también aparezcan en la lista de direcciones permitidas.

Nombre de la lista: especifique el nombre de la lista. Este campo aparecerá en gris cuando se edite una de las tres listas predefinidas.

Descripción de la lista: escriba una breve descripción de la lista (opcional). Aparecerá en gris cuando se edite una de las tres listas predefinidas.

Para activar una lista, seleccione **Lista activa** junto a esa lista. Si desea recibir una notificación cuando se use una lista específica en la evaluación de un sitio HTTP que usted visitó, seleccione **Notificar al aplicar**. Por ejemplo, se emitirá una notificación si un sitio web está bloqueado o permitido por estar incluido en una lista de direcciones bloqueadas o permitidas. Esta notificación incluirá el nombre de la lista que contiene el sitio web especificado.

Agregar: agregue una dirección URL nueva a la lista (ingrese múltiples valores con separadores).

Editar: modifica la dirección existente en la lista. Solo es posible para las direcciones creadas con Agregar.

Quitar: elimina las direcciones existentes en la lista. Solo es posible para las direcciones creadas con Agregar.

Importar: importe un archivo con direcciones URL (valores separados por un salto de línea; por ejemplo, *.txt, cuando use codificación UTF-8).

4.4.4.2.2 Lista de direcciones

En esta sección, puede especificar las listas de direcciones HTTP que se bloquearán, permitirán o excluirán de la verificación.

De forma predeterminada, se pueden usar estas tres listas:

- **Lista de direcciones excluidas de la verificación:** no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones permitidas:** si se habilita **Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas**, y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones que se encuentran en esta lista. Las direcciones de esta lista se permiten incluso si están incluidas en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas :** el usuario no tendrá acceso a las direcciones especificadas en esta lista, a menos que también aparezcan en la lista de direcciones permitidas.

Haga clic en **Agregar...** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Quitar**.

4.4.5 Protección Anti-Phishing

ESET Mail Security también ofrece protección contra suplantación de identidad. La protección Anti-Phishing es parte del módulo de correo electrónico e Internet. Si ha instalado ESET Mail Security utilizando el tipo de [instalación completa](#), Internet y correo electrónico se instalan de manera predeterminada con la protección Anti-Phishing activada. Sin embargo, esto no se aplica a sistemas que ejecutan Microsoft Windows Server 2008.

NOTA

el componente de Internet y correo electrónico no es parte del tipo de instalación **Completa** ESET Mail Security en los sistemas Windows Server 2008 o Windows Server 2008 R2. Si se requiere, puede modificar la instalación existente agregando el componente de Internet y correo electrónico para poder utilizar la protección Anti-Phishing.

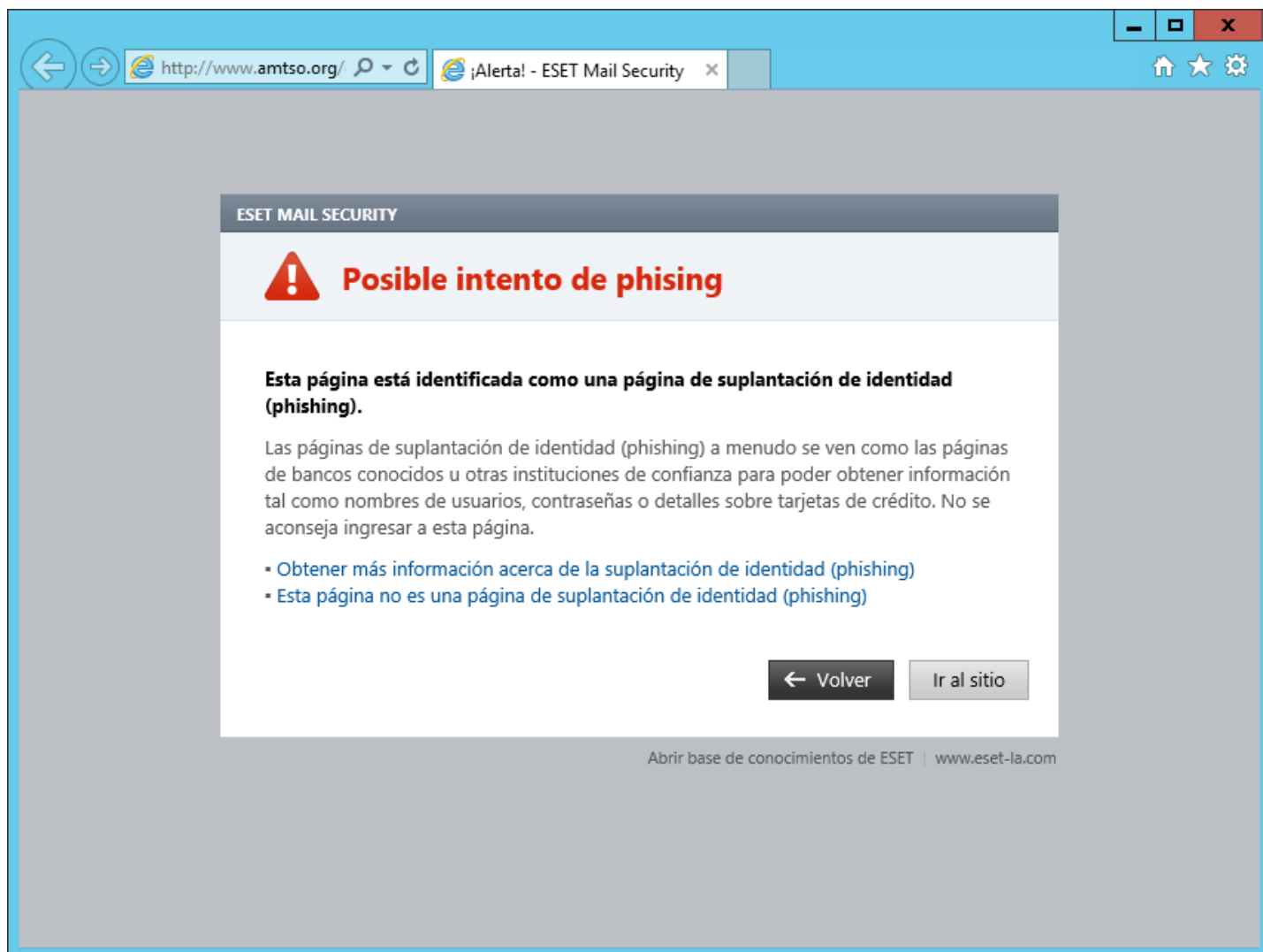
El término phishing define una actividad criminal que usa la ingeniería social (manipula a los usuarios para obtener información confidencial). El phishing suele usarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc. Obtenga más información sobre esta actividad en el [glosario](#). ESET Mail Security incluye protección antiphishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido.

Se recomienda firmemente habilitar Anti-Phishing en ESET Mail Security. Para hacerlo, abra **Configuración avanzada** (F5) y vaya a **Internet y correo electrónico > Protección Anti-Phishing**.

Visite nuestro [Artículo de la base de conocimiento](#) para obtener más información acerca de la protección antiphishing en ESET Mail Security.

Acceso a un sitio web de phishing

Cuando accede a un sitio web de phishing reconocido, se mostrará el siguiente diálogo en su navegador web. Si aún desea acceder al sitio web, haga clic en **Ir al sitio** (no recomendado).



i NOTA

Los posibles sitios web de phishing de la lista blanca se vencerán, de forma predeterminada, luego de algunas horas. Para permitir un sitio web de manera permanente, use la herramienta [Administración de direcciones URL](#). En **Configuración avanzada** (F5) expanda **Internet y correo electrónico** > **Protección del acceso web** > **Administración de direcciones URL** > **Lista de direcciones**, haga clic en **Editar**, y luego agregue a la lista el sitio web que desea editar.

Informe de un sitio de phishing

El vínculo [Informar](#) le permite informar a ESET los sitios web maliciosos o de phishing que deben analizarse.

i NOTA

antes de enviar un sitio web a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:

- el programa directamente no detecta el sitio web
- el programa detecta erróneamente el sitio usar como una amenaza. En este caso, puede [Informar un sitio de phishing falso positivo](#).

Como alternativa, puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Recuerde usar un asunto descriptivo y proporcionar la mayor cantidad de información posible sobre el sitio web (por ejemplo, el sitio web que se lo recomendó, cómo se enteró de este sitio web, etc.).

4.5 Control del dispositivo

ESET Mail Security proporciona el control del dispositivo automático (CD/DVD/USB/). Este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado. Resulta útil si el administrador del equipo desea prevenir el uso de dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (HDD, disco USB extraíble)
- CD/DVD
- Impresora USB
- Almacenamiento FireWire
- Dispositivo Bluetooth
- Lector de tarjeta inteligente
- Dispositivo de imagen
- Módem
- Puerto LPT/COM
- Dispositivo portátil
- Todos los tipos de dispositivos

Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración avanzada** (F5) > **Control del dispositivo**.

Cuando habilita el interruptor ubicado junto a **Integrar al sistema**, se activa la característica de Control del dispositivo en ESET Mail Security; deberá reiniciar el equipo para que se aplique este cambio. Una vez que se habilita el Control del dispositivo, se activará el **Editor de reglas**, lo cual le permite abrir la ventana [Editor de reglas](#).

Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación y no se otorgará el acceso al dispositivo.

4.5.1 Control del dispositivo: editor de reglas

La ventana **Editor de reglas del control del dispositivo** muestra las reglas existentes y permite el control preciso de dispositivos externos que los usuarios conectan al equipo.

Reglas

Nombre	Habilitado	Tipo	Descripción	Acción	Usuarios	Severidad
Block USB for User	<input checked="" type="checkbox"/>	Dispositivo portátil		Bloquear	Todos	Siempre

Agregar

Editar

Copiar

Quitar

Llenar

Aceptar

Cancelar

Los dispositivos específicos pueden ser permitidos o bloqueados por el usuario, el grupo de usuarios, o cualquiera de los varios parámetros adicionales que se pueden especificar en la configuración de reglas. La lista de reglas contiene varias descripciones de una regla como nombre, tipo de dispositivo externo, acción a realizar después de conectar un dispositivo externo en su equipo y la severidad del registro.

- Haga clic en **Agregar** o **Editar** para administrar una regla. Haga clic en **Quitar** si desea eliminar la regla seleccionada o anule la selección de la casilla de verificación **Habilitada** que se encuentra junto a la regla en particular para deshabilitarla. Esto puede ser útil si no desea eliminar una regla en forma permanente, para poder usarla en el futuro.
- **Copiar**: crea una regla nueva basada en los parámetros de la regla seleccionada.
- Haga clic en **Llenar** para completar automáticamente los parámetros de los dispositivos de medios extraíbles conectados al equipo.
- Las reglas se incluyen en la lista por orden de prioridad, con las reglas de prioridad más alta más cerca de la parte superior. Puede seleccionar varias reglas y aplicar acciones, tal como eliminarlas o moverlas hacia arriba o abajo en la lista, al hacer clic en **Superior/Arriba/Abajo/Inferior** (botones de flechas).

Puede ver las entradas de registro desde la ventana principal del programa de ESET Mail Security en **Herramientas > Archivos de registro**.

4.5.2 Agregado de reglas del control del dispositivo

Una regla de control del dispositivo define la acción que se tomará cuando un dispositivo, que cumple con los criterios de las reglas, se conecte al equipo.

Editar regla

?

Nombre

Block USB for User

Regla habilitada

☒

Tipo de dispositivo

Dispositivo portátil

Acción

Bloquear

Tipo de criterios

Dispositivo

Proveedor

Modelo

Número de serie

Severidad de registros

Siempre

Lista de usuarios

Editar

Aceptar

Ingrese una descripción de la regla en el campo **Nombre** para tener una mejor identificación. Haga clic en el interruptor junto a **Regla habilitada** para deshabilitar o habilitar esta regla; esto puede ser útil si no desea eliminar la regla permanentemente.

Tipo de dispositivo

Elija el tipo de dispositivo externo desde el menú desplegable (Almacenamiento en disco/Dispositivo portátil/Bluetooth/FireWire/...). Los tipos de dispositivos se heredan del sistema operativo y se pueden ver en el administrador de dispositivos del sistema siempre y cuando un dispositivo esté conectado al equipo. Los dispositivos de almacenamiento incluyen los discos externos o los lectores de tarjetas de memoria convencionales conectados por medio de USB o FireWire. Los lectores de tarjetas inteligentes incluyen todos los lectores de tarjetas inteligentes con un circuito integrado, tal como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras; estos dispositivos no proporcionan información sobre usuarios, únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

Acción

El acceso a los dispositivos que no son de almacenamiento se puede permitir o bloquear. Por el contrario, las reglas para los dispositivos de almacenamiento le permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/escritura:** se permitirá el acceso total al dispositivo.
- **Bloquear:** se bloqueará el acceso al dispositivo.
- **Solo lectura:** solo se permitirá el acceso de lectura al dispositivo.
- **Advertir:** siempre que se conecte un dispositivo, se le notificará al usuario si está permitido/bloqueado, y se

generará una entrada de registro. Los dispositivos no se recuerdan, pero aún se mostrará una notificación en las conexiones posteriores del mismo dispositivo.

Observe que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivo. Si un dispositivo tiene espacio de almacenamiento, las cuatro acciones estarán disponibles. Para los dispositivos de no almacenamiento, solo existen dos (por ejemplo, la acción **Solo lectura** no está disponible para Bluetooth, entonces los dispositivos Bluetooth solo se pueden permitir o bloquear).

Los parámetros adicionales que figuran a continuación se pueden usar para ajustar las reglas y personalizarlas para los dispositivos. Todos los parámetros no distinguen entre mayúsculas y minúsculas:

- **Proveedor:** filtre por nombre o ID del proveedor.
- **Modelo:** el nombre determinado del dispositivo.
- **Número de serie:** los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.

i NOTA

si estos tres descriptores están vacíos, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado en todos los campos de texto no distinguen mayúsculas de minúsculas y no aceptan caracteres globales (*, ?).

con el fin de descifrar los parámetros de un dispositivo, cree una regla para permitir ese el tipo de dispositivo, conecte el dispositivo a su equipo y luego revise los detalles del dispositivo en el [Registro de control del dispositivo](#).

Gravedad

- **Siempre:** registra todos los eventos.
- **Diagnóstico:** registra la información necesaria para ajustar el programa.
- **Información:** registra los mensajes de información, incluidos los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencia:** registra los errores críticos y mensajes de advertencia.
- **Ninguno :** no se realizará registro alguno.

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la **Lista de usuarios**:

- **Agregar:** abre los **Tipos de objetos: usuarios o grupos** que permite seleccionar los usuarios deseados.
- **Quitar:** quita el usuario seleccionado del filtro.

i NOTA

todos los dispositivos se pueden filtrar por reglas del usuario, (por ejemplo: los dispositivos de imagen no proporcionan información sobre usuarios, únicamente sobre acciones invocadas).

4.5.3 Dispositivos detectados

El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con la siguiente información: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible). Cuando seleccione un dispositivo (en la lista de Dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede ajustar todas las configuraciones).

4.5.4 Grupos de dispositivos

ADVERTENCIA

El dispositivo conectado a su equipo puede presentar un riesgo de seguridad.

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo respectivo, y la parte izquierda de la ventana contiene una lista de los grupos existentes. Seleccione el grupo que contiene los dispositivos que desea mostrar en el panel derecho.

Cuando abre la ventana Grupos de dispositivos y selecciona un grupo, puede agregar o eliminar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. Como alternativa, puede hacer clic en **Llenar**, y todos los dispositivos conectados a su equipo se incluirán en una lista en la ventana **Dispositivos detectados**. Seleccione un dispositivo de la lista que se completó para agregarlo al grupo haciendo clic en **ACEPTAR**.

NOTA

Puede crear distintos grupos de dispositivos para los que se aplicarán reglas diferentes. También puede crear solo un grupo de dispositivos para el que se aplicará la regla con la acción **Lectura/Escritura** o **Solo lectura**. Esto garantiza que el Control de dispositivos bloqueará los dispositivos no reconocidos cuando se conectan a su equipo.

Elementos de control

- **Agregar:** puede agregar un grupo al ingresar su nombre, o un dispositivo a un grupo existente. (de forma opcional, puede especificar los detalles como el nombre del proveedor, el modelo y el número de serie) dependiendo de la parte de la ventana en la que haya hecho clic en el botón.
- **Editar:** le permite modificar el nombre de un grupo seleccionado o los parámetros de los dispositivos contenidos allí (proveedor, modelo, número de serie).
- **Eliminar:** elimina el grupo o el dispositivo seleccionado, dependiendo de la parte de la ventana en la que haya hecho clic.
- **Importar:** importa una lista de dispositivos desde un archivo.
- El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con la siguiente información: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible).

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea salir de la ventana **Grupos de dispositivos** sin guardar los cambios.

NOTA

Tenga en cuenta que no todas las Acciones (permisos) están disponibles para todos los tipos de dispositivos. Para los dispositivos de almacenamiento, las cuatro acciones están disponibles. Para los dispositivos de no almacenamiento, solo hay tres Acciones disponibles (por ejemplo, **Solo lectura** no está disponible para Bluetooth, por lo que los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

4.6 Herramientas

La siguiente es la configuración avanzada para todas las herramientas que ESET Mail Security ofrece en la pestaña **Herramientas** en la ventana de la interfaz gráfica principal del usuario.

4.6.1 ESET LiveGrid

<%ELG%> es un sistema avanzado de alerta temprana compuesto por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes en base a la reputación y mejora el rendimiento de las exploraciones por medio de las listas blancas. La información de la amenaza nueva se transmite en tiempo real a la nube, lo que le permite al Laboratorio de búsqueda de malware de ESET proporcionar una respuesta oportuna y una protección consistente en todo momento. Los usuarios pueden verificar la reputación de los procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual, con información adicional disponible desde <%ELG%>. Cuando instale ESET Mail Security, seleccione una de las siguientes opciones:

1. Puede decidir no habilitar <%ELG%>. Su software no perderá funcionalidad alguna pero, en algunos casos, ESET Mail Security puede responder más lento a las nuevas amenazas que una actualización de la base de datos de firmas de virus.
2. Puede configurar <%ELG%> para enviar información anónima sobre las amenazas nuevas y el contexto donde se detectó dicho código. Es posible enviar este archivo a ESET para su análisis detallado. El estudio de estos códigos ayudará a ESET a actualizar su capacidad de detección de amenazas.

<%ELG%> recopilará información sobre el equipo en relación con las nuevas amenazas detectadas. Dicha información puede incluir una muestra o copia del archivo donde apareció la amenaza, la ruta a ese archivo, el nombre del archivo, la fecha y la hora, el proceso mediante el cual apareció la amenaza y la información sobre el sistema operativo del equipo.

En forma predeterminada, ESET Mail Security está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis detallado. Los archivos con ciertas extensiones, como .doc o .xls, siempre se excluyen. También puede agregar otras extensiones si usted o su organización prefieren no enviar ciertos archivos específicos.

El sistema de reputación <%ELG%> proporciona listas blancas y negras basadas en la nube. Para acceder a la configuración de <%ELG%>, presione la tecla F5 para ingresar a “Configuración avanzada” y expanda **Herramientas > <%ELG%>**.

Habilitar el sistema de reputación <%ELG%> (recomendado): el sistema de reputación <%ELG%> mejora la eficacia de las soluciones antimalware de ESET al comparar los archivos analizados con una base de datos de elementos de listas blancas y negras en la nube.

Enviar estadísticas anónimas: permita a ESET recopilar información acerca de amenazas detectadas recientemente como el nombre de la amenaza, la fecha y la hora de detección, el método de detección y los metadatos asociados, la versión del producto, y la configuración, incluida la información sobre su sistema.

Enviar archivos: los archivos sospechosos que se asemejan a amenazas, y/o los archivos con características o comportamientos inusuales se envían a ESET para su análisis.

Seleccione **Habilitar la creación de registros** para crear un registro de sucesos que recopile información sobre los archivos y los datos estadísticos enviados. Esto permite la creación de registros en el [Registro de sucesos](#) cuando se envían los archivos o datos estadísticos.

Correo electrónico de contacto (opcional): puede incluir su correo electrónico junto con los archivos sospechosos, así podrá usarse para contactarlo en caso de que se requiera información adicional para el análisis. Recuerde que no recibirá ninguna respuesta de ESET a menos que se necesite información adicional.

Exclusiones: el filtro de exclusión le permite excluir ciertos archivos o ciertas carpetas del envío (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Los tipos de archivos más comunes se excluyen en forma predeterminada (.doc, etc.). Si lo desea, puede agregar archivos a la lista de archivos excluidos.

Si usted ya usó <%ELG%> y lo deshabilitó, es posible que queden paquetes de datos para enviar. Aun después de su desactivación, dichos paquetes se enviarán a ESET. Una vez que se envíe toda la información actual, no se crearán más paquetes.

4.6.1.1 Filtro de exclusión

La opción **Editar** junto a Exclusiones en <%ELG%> le permite configurar la manera en que las amenazas se envían a los laboratorios de virus de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio de amenazas para su análisis. Si se trata de una aplicación maliciosa, se agregará su detección en la siguiente actualización de firmas de virus.

4.6.2 Cuarentena

Los archivos infectados o sospechosos se almacenan con una apariencia inofensiva en la carpeta de cuarentena. En forma predeterminada, el módulo de protección en tiempo real pone en cuarentena todos los nuevos archivos sospechosos creados para evitar la infección.

Volver a explorar los archivos en cuarentena luego de cada actualización: se explorarán todos los objetos en cuarentena luego de cada actualización de la base de datos de firmas de virus. Esto es especialmente útil si se ha enviado un archivo a cuarentena como consecuencia de la detección de un [falso positivo](#). Con esta opción habilitada, ciertos tipos de archivos se pueden restaurar automáticamente a su ubicación original.

4.6.3 Actualización de Microsoft Windows

Las actualizaciones de Windows proporcionan las reparaciones importantes para las vulnerabilidades potencialmente peligrosas y mejoran el nivel general de seguridad en su equipo. Por ese motivo, es imprescindible instalar las actualizaciones de Microsoft Windows en cuanto estén disponibles. ESET Mail Security lo mantendrá notificado sobre las actualizaciones faltantes según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones:** no se ofrecerá la descarga de ninguna actualización del sistema.
- **Actualizaciones opcionales:** las actualizaciones marcadas como de baja prioridad y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones recomendadas:** las actualizaciones marcadas como comunes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones importantes:** las actualizaciones marcadas como importantes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones críticas:** solo se ofrecerá la descarga de las actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará tras la verificación del estado con el servidor de actualización. Es posible que la información de actualización del sistema no esté disponible de inmediato después de guardar los cambios.

4.6.4 Proveedor WMI

Acerca de WMI

La Instrumentación para la administración de Windows (WMI) es la implementación de Microsoft de Web-Based Enterprise Management (WBEM, gestión de empresa basada en la web), una iniciativa de la industria para desarrollar una tecnología estándar para acceder a la información de gestión en un entorno empresarial.

Para obtener más información sobre WMI, consulte [http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx)

Proveedor WMI de ESET

El propósito del Proveedor WMI de ESET es permitir la supervisión remota de los productos de ESET en un entorno empresarial sin necesitar ningún software o herramientas específicos de ESET. Al exponer la información del producto básico, el estado y las estadísticas a través de WMI, ampliamos considerablemente las posibilidades de los administradores empresariales en la supervisión de los productos de ESET. Los administradores pueden aprovechar el número de métodos de acceso que WMI ofrece (línea de comandos, scripts y herramientas de supervisión empresarial de terceros) para supervisar el estado de sus productos de ESET.

La implementación actual proporciona acceso de solo lectura para la información básica del producto, las funciones

instaladas y su estado de protección, las estadísticas de exploraciones individuales y los archivos de registro de los productos.

El proveedor de WMI permite el uso de la infraestructura y las herramientas estándar de Windows WMI para leer el estado del producto y de los registros del producto.

4.6.4.1 Datos proporcionados

Todas las clases de WMI relacionadas con el producto de ESET se encuentran en el espacio de nombres “raíz/ESET”. Las siguientes clases, que se describen en detalle a continuación, están implementadas actualmente:

General:

- ESET_Product
- ESET_Features
- ESET_Statistics

Registros:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

Clase ESET_Product

Solo puede haber una instancia para la clase ESET_Product. Las propiedades de esta clase se refieren a la información básica sobre su producto de ESET instalado:

- **ID:** identificador del tipo de producto, por ejemplo, “essbe”
- **Name:** nombre del producto, por ejemplo, “ESET Security”
- **Edition:** edición del producto, por ejemplo, “Microsoft SharePoint Server”
- **Version:** versión del producto, por ejemplo, “4.5.15013.0”
- **VirusDBVersion:** versión de la base de datos de virus, por ejemplo, “7868 (20130107)”
- **VirusDBLastUpdate:** fecha y hora de la última actualización de la base de datos de virus. La cadena contiene la fecha y la hora en el formato de fecha y hora de WMI, por ejemplo, “20130118115511.000000+060”
- **LicenseExpiration:** tiempo de expiración de la licencia. La cadena contiene la fecha y la hora en el formato de fecha y hora de WMI, por ejemplo, “20130118115511.000000+060”
- **KernelRunning:** valor booleano que indica si el servicio eKrnestá funcionando en el equipo, por ejemplo, “VERDADERO”
- **StatusCode:** el número que indica el estado de protección del producto: 0 - Verde (bueno), 1 - Amarillo (advertencia), 2 - Rojo (error)
- **StatusText:** mensaje que describe la razón de un código de estado distinto de cero, de lo contrario es nulo

Clase ESET_Features

La clase ESET_Features tiene instancias múltiples, según el número de características del producto. Cada instancia contiene:

- **Name:** nombre de la característica (la lista de nombres se proporciona a continuación)
- **Status:** estado de la característica: 0 - inactiva, 1 - deshabilitada, 2 - habilitada

Una lista de cadenas que representan las características de productos reconocidas actualmente:

- **CLIENT_FILE_AV**: protección antivirus del sistema de archivos en tiempo real
- **CLIENT_WEB_AV**: protección antivirus del cliente de Internet
- **CLIENT_DOC_AV**: protección antivirus de los documentos del cliente
- **CLIENT_NET_FW**: firewall personal del cliente
- **CLIENT_EMAIL_AV**: protección antivirus de clientes de correo electrónico
- **CLIENT_EMAIL_AS**: protección antispam de clientes de correo electrónico
- **SERVER_FILE_AV**: protección antivirus en tiempo real de archivos en el producto de servidor de archivos protegido, por ejemplo, archivos de base de datos de contenido de SharePoint en el caso de ESET Mail Security
- **SERVER_EMAIL_AV**: protección antivirus de correos electrónicos de productos de servidores protegidos, por ejemplo, correos electrónicos en MS Exchange o IBM Domino
- **SERVER_EMAIL_AS**: protección antispam de correos electrónicos de productos de servidores protegidos, por ejemplo, correos electrónicos en MS Exchange o IBM Domino
- **SERVER_GATEWAY_AV**: protección antivirus de los protocolos de red protegidos en la puerta de enlace
- **SERVER_GATEWAY_AS** - protección antispam de los protocolos de red protegidos en la puerta de enlace

Clase ESET_Statistics

La clase ESET_Statistics tiene instancias múltiples, según el número de exploraciones en el producto. Cada instancia contiene:

- **Scanner**: código de cadena para la exploración específica, por ejemplo, "CLIENT_FILE"
- **Total**: número total de archivos explorados
- **Infected**: número de archivos infectados que se encontraron
- **Cleaned**: número de archivos desinfectados
- **Fecha y hora**: la fecha y la hora del último cambio de esta estadística. En un formato de fecha y hora de WMI, por ejemplo, "20130118115511.000000+060"
- **ResetTime**: fecha y hora en que se reinició por última vez el contador de estadísticas. En un formato de fecha y hora de WMI, por ejemplo, "20130118115511.000000+060"

Lista de cadenas que representan las exploraciones reconocidas actualmente:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Clase ESET_ThreatLog

La clase ESET_ThreatLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro "Amenazas detectadas". Cada instancia contiene:

- **ID**: identificación única de este historial de registros
- **Timestamp**: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel**: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner**: nombre de la exploración que creó este evento de registro
- **ObjectType**: tipo de objeto que produjo este evento de registro
- **ObjectName**: nombre del objeto que produjo este evento de registro
- **Threat**: nombre de la amenaza encontrada en el objeto descrito por las propiedades de ObjectName y ObjectType
- **Action**: acción realizada luego de identificar la amenazada
- **User**: cuenta de usuario que causó la generación de este evento de registro
- **Information**: descripción adicional del evento

ESET_EventLog

La clase ESET_EventLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Eventos”. Cada instancia contiene:

- **ID:** identificación única de este historial de registros
- **Timestamp:** fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel:** gravedad del historial de registros expresada como un número en el intervalo de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module:** nombre del módulo que creó este evento de registro
- **Event:** descripción del evento
- **User:** cuenta de usuario que causó la generación de este evento de registro

ESET_ODFileScanLogs

La clase ESET_ODFileScanLogs tiene instancias múltiples, cada una de las cuales representa un registro de exploración de archivos a petición. Esto equivale a la lista de registros “Exploración del equipo a petición” de la GUI. Cada instancia contiene:

- **ID:** identificación única de este registro a petición
- **Timestamp:** fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- **Targets:** carpetas/objetos de destino de la exploración
- **TotalScanned:** número total de objetos explorados
- **Infected:** número de objetos infectados encontrados
- **Cleaned:** número de objetos desinfectados
- **Status:** estado del proceso de exploración

ESET_ODFileScanLogRecords

La clase ESET_ODFileScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_ODFileScanLogs. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones a petición. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia de clase contiene:

- **LogID:** identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_ODFileScanLogs)
- **ID:** identificación única de este historial de registros de exploración
- **Timestamp:** fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel:** gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log:** el mensaje de registro real

ESET_ODServerScanLogs

La clase ESET_ODServerScanLogs tiene instancias múltiples, cada una de las cuales representa una ejecución de la exploración del servidor a petición. Cada instancia contiene:

- **ID:** identificación única de este registro a petición
- **Timestamp:** fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- **Targets:** carpetas/objetos de destino de la exploración
- **TotalScanned:** número total de objetos explorados
- **Infected:** número de objetos infectados encontrados
- **Cleaned:** número de objetos desinfectados
- **RuleHits:** número total de objetos explorados
- **Status:** estado del proceso de exploración

ESET_ODServerScanLogRecords

La clase ESET_ODServerScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_ODServerScanLogs. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones a petición. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia de clase contiene:

- **LogID:** identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_ODServerScanLogs)
- **ID:** identificación única de este historial de registros de exploración
- **Timestamp:** fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel:** gravedad del historial de registros expresada como un número en el intervalo de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log:** el mensaje de registro real

ESET_GreylistLog

La clase ESET_GreylistLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro "Listado gris". Cada instancia contiene:

- **ID:** identificación única de este historial de registros
- **Timestamp:** fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel:** gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain:** nombre del dominio HELO
- **IP:** dirección IP de origen
- **Sender:** remitente de correo electrónico
- **Recipient:** destinatario de correo electrónico
- **Action:** acción realizada
- **TimeToAccept:** número de minutos después de los que se aceptará el correo electrónico

ESET_SpamLog

La clase ESET_SpamLog tiene instancias múltiples, cada una de las cuales representa un historial de registros "Spamlog". Cada instancia contiene:

- **ID:** identificación única de este historial de registros
- **Timestamp:** fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- **LogLevel:** gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sender:** remitente de correo electrónico
- **Recipients:** destinatarios de correo electrónico
- **Subject:** asunto del correo electrónico
- **Received:** hora de recepción
- **Score:** puntaje de spam en porcentaje [0-100]
- **Reason:** motivo por el cual este correo electrónico se marcó como spam
- **Action:** acción realizada
- **DiagInfo:** información de diagnóstico adicional

4.6.4.2 Acceso a los datos proporcionados

Aquí hay algunos ejemplos de cómo acceder a los datos WMI de ESET desde la línea de comandos de Windows y PowerShell, que deben funcionar desde cualquier sistema operativo actual de Windows. Sin embargo, hay muchas otras maneras de acceder a los datos desde otros lenguajes y herramientas de scripting.

Línea de comandos sin scripts

El menú`wmic` herramienta de línea de comandos puede usarse para acceder a cualquier clase de WMI personalizada o a algunas predefinidas.

Para mostrar toda la información sobre el producto en el equipo local:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Para mostrar el número de versión del producto solo del producto en el equipo local:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Para mostrar toda la información sobre el producto en un equipo remoto con IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Para mostrar y obtener toda la información sobre el producto en el equipo local:

```
Get-WmiObject ESET_Product -namespace "root\ESET"
```

Para mostrar y obtener toda la información sobre el producto en un equipo remoto con IP 10.1.118.180:

```
$cred = Get-Credential # solicita al usuario las credenciales y las almacena en la variable  
Get-WmiObject ESET_Product -namespace "root\ESET" -computername "10.1.118.180" -cred $cred
```

4.6.5 Objetivos para explorar de ERA

Esta funcionalidad le permite al [ESET Remote Administrator](#) utilizar objetivos de exploración de la base de datos a petición apropiados cuando se ejecuta la tarea de cliente **Exploración del servidor** en un servidor con ESET Mail Security.

Cuando habilita la funcionalidad **Generar lista de objetivos**, ESET Mail Security crea una lista de los objetivos para explorar actualmente disponibles de la base de datos. Esta lista se genera periódicamente, según cómo se defina en **Períodos de actualización** en minutos. Cuando ERA quiere ejecutar una tarea en el cliente de **Exploración del servidor**, recogerá la lista y le permitirá elegir los objetos para explorar con el explorador bajo demanda de la base de datos en ese servidor en particular.

4.6.6 Archivos de registro

Esta sección le permite modificar la configuración de registro de ESET Mail Security. Puede usar los interruptores para deshabilitar o habilitar una función en particular. Para iniciar el registro real, debe activar el registro de diagnóstico general a nivel del producto desde el menú principal > **Configuración** > [Herramientas](#). Una vez que el mismo registro está activado, ESET Mail Security recopilará los registros detallados según las características que están habilitadas en esta sección. Todos los registros están escritos en el registro de **Eventos** (C:\ProgramData\ESET\ESET Mail Security\Logs\warnlog.dat) y se pueden visualizar en el visor de [Archivos de registro](#).

Historiales de registros

Registro de errores de transporte del correo electrónico: si esta opción está habilitada y existen problemas en la capa de transporte de correo electrónico, los mensajes de error se escriben en el registro de Eventos.

Excepciones del registro de transporte de correo electrónico: si existe alguna excepción en la capa de transporte de correo electrónico, se escribirán los detalles acerca de la misma en el registro de Eventos.

Registro de diagnósticos

Registro de diagnóstico de la protección de la base de datos

Registro de diagnóstico del transporte de correo

Registro del diagnóstico de la exploración de la base de datos a petición

Registro de diagnóstico de clúster: puede usar el interruptor para deshabilitar o habilitar el **Registro de diagnóstico de clúster** de ser necesario. En forma predeterminada, se encuentra habilitado. Esto significa que el registro de

clúster se incluirá en el registro de diagnóstico general.

Archivos de registro: puede definir cómo se administrarán los registros. El programa elimina en forma automática los registros más antiguos para ahorrar espacio en el disco.

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO 1

HERRAMIENTAS

Archivos de registro

Servidor proxy

Notificaciones por correo electrónico

Modo de presentación

Diagnósticos

Clúster

INTERFAZ DEL USUARIO

ARCHIVOS DE REGISTRO

Eliminar automáticamente historiales anteriores a (días) ☒ 90

Elimine automáticamente los historiales antiguos, si se excede el tamaño de los registros ☒

Tamaño máx. de registros [MB] 50

Tamaño de registros reducido [MB] 30

Realizar copias de seguridad de los historiales eliminados automáticamente ☐

Realizar copias de seguridad de los registros de diagnóstico ☐

Carpeta de copias de seguridad

Comprima las copias de seguridad de los registros con el uso del ZIP ☒

Optimizar archivos de registro automáticamente ☒

Predeterminado Aceptar Cancelar

Las entradas de registro más antiguas que el número de días especificados en el campo **Eliminar automáticamente los registros más antiguos que (días)** se borrarán automáticamente.

Eliminar automáticamente historiales antiguos si se excede el tamaño de los registros: cuando el tamaño de los registros excede el **Tamaño máx. de registros [MB]**, se eliminarán los registros antiguos hasta que se alcance un **Tamaño de registros reducido [MB]**.

Realizar copias de seguridad de los historiales eliminados automáticamente: se realizarán copias de seguridad de los archivos e historiales de registros eliminados automáticamente en un directorio especificado y con la opción de comprimirlo en archivos ZIP

Realizar copias de seguridad de los registros de diagnóstico: realizará copias de seguridad de registros de diagnóstico eliminados automáticamente. Si no están habilitados, no se harán copias de seguridad de los historiales de registros de diagnóstico.

Carpeta de copias de seguridad: carpeta donde se almacenarán las copias de seguridad de los registros. Puede habilitar las **copias de seguridad de los registros comprimidos con el uso de ZIP**.

Optimizar archivos de registro automáticamente: si está activada, se desfragmentarán automáticamente los archivos de registro si el porcentaje de fragmentación es mayor al valor especificado en el campo **Si la cantidad de registros no usados excede (%)**.

Haga clic en **Optimizar archivos de registro** para comenzar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan para mejorar el rendimiento y la velocidad de procesamiento del registro. Esta mejora se observa más claramente cuanto mayor es el número de entradas de los registros.

Active **Habilitar protocolo de texto** para habilitar el almacenamiento de los registros en otro formato de archivo separado de los [Archivos de registro](#):

- **Directorio de destino:** es el directorio donde se almacenarán los archivos de registro (solo se aplica a texto/CSV). Cada sección de registro tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, *virlog.txt*)

para la sección de archivos de registro **Amenazas detectadas**, si usa un formato de archivo de texto sin formato para almacenar los registros).

- **Tipo:** si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto; los datos se separarán mediante tabulaciones. Lo mismo se aplica para el formato del archivo **CSV** separado con comas. Si elige **Evento**, los registros se almacenarán en el registro Windows Event (se puede ver mediante el Visor de eventos en el Panel de control) en lugar del archivo.

Eliminar todos los archivos de registro: borra todos los registros almacenados seleccionados en el menú desplegable **Tipo**.

4.6.6.1 Filtrado de registros

Registra información sobre sucesos importantes del sistema. La característica de filtrado de registros permite ver los registros de un tipo específico de suceso.

Ingrese la palabra clave de búsqueda en el campo **Buscar el texto**. Use el menú desplegable **Buscar en columnas** para perfeccionar su búsqueda.

Tipos de historiales: elija un tipo de historial de registro o varios desde el menú desplegable:

- **Diagnóstico:** registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo:** registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias:** registra los errores críticos y los mensajes de advertencia.
- **Errores:** se registrarán errores tales como "Error al descargar el archivo" y los errores críticos.
- **Crítico:** registra solo los errores críticos (error al iniciar la protección antivirus).

Período: defina el momento a partir del cual desea que se muestren los resultados.

Solo coincidir palabras completas: seleccione esta casilla de verificación si desea buscar palabras completas específicas para obtener resultados más precisos.

Coincidir mayúsculas y minúsculas: habilite esta opción si para usted es importante distinguir entre mayúsculas y minúsculas en el filtrado.

4.6.6.2 Búsqueda en el registro

Además del [Filtrado de registros](#), se puede usar la función de búsqueda dentro de los archivos de registro, aunque también puede usarse en forma independiente del filtrado de registros. Esta función es útil cuando se están buscando historiales específicos en los registros. Al igual que el Filtrado de registros, esta característica de búsqueda lo ayudará a encontrar la información que busca, en particular cuando hay demasiados historiales.

Cuando busque en el registro, puede **Buscar texto** al escribir una cadena específica, use el menú desplegable **Buscar en columnas** para filtrar por columna, seleccione **Tipos de historiales** y establezca un **Período** para buscar solo los historiales de un período de tiempo específico. Al especificar ciertas opciones de búsqueda, solo se buscarán los historiales relevantes (según esas opciones de búsqueda) en la ventana Archivos de registro.

Buscar el texto: Escriba una cadena (una palabra o parte de una palabra). Solo se buscarán los historiales que contengan la cadena de texto especificada. Se omitirán otros historiales.

Buscar en columnas: Seleccione qué columnas se tendrán en cuenta durante la búsqueda. Se pueden seleccionar una o más columnas para usar en la búsqueda. De forma predeterminada, se seleccionan todas las columnas:

- Hora
- Carpeta explorada
- Suceso
- Usuario

Tipos de historiales: Elija un tipo de historial de registro o varios desde el menú desplegable:

- **Diagnóstico:** registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo:** registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias:** registra los errores críticos y los mensajes de advertencia.
- **Errores:** se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico:** registra solo los errores críticos (error al iniciar la protección antivirus).

Período: Defina el período a partir del cual desea que se muestren los resultados.

- **No especificado** (predeterminado): no busca en el período especificado, ya que busca en el registro completo.
- **Ayer**
- **La semana pasada**
- **El mes pasado**
- **Período:** puede especificar el período exacto (fecha y hora) para buscar solo aquellos historiales de un período específico.

Solo coincidir palabras completas: encuentra únicamente los historiales que contienen palabras completas coincidentes con la cadena de texto ingresada en el campo **Texto**.

Coincidir mayúsculas y minúsculas: encuentra únicamente los historiales que contienen palabras coincidentes con la cadena de texto ingresada en el campo **Texto**, respetando el uso de mayúsculas y minúsculas.

Buscar hacia arriba: busca desde la posición actual hacia arriba.

Cuando haya configurado las opciones de búsqueda, haga clic en **Buscar** para iniciar la búsqueda. La búsqueda se detiene al encontrar el primer historial coincidente. Haga clic otra vez en **Buscar** para ver historiales adicionales. Los archivos de registro se buscan desde arriba hacia abajo, comenzando desde la posición actual (el historial resaltado).

4.6.7 Servidor proxy

En redes de área local muy extensas, la conexión del equipo a Internet puede tener como intermediario un servidor proxy. En tal caso, será necesario definir las siguientes opciones de configuración. De lo contrario, el programa no podrá actualizarse en forma automática. En ESET Mail Security, la configuración del servidor proxy está disponible en dos secciones diferentes del árbol de configuración avanzada.

Primero, la configuración del servidor proxy puede establecerse en **Configuración avanzada** en **Herramientas > Servidor proxy**. La especificación del servidor proxy en esta etapa define la configuración global del servidor proxy para todo ESET Mail Security. Todos los módulos que requieran una conexión a Internet usarán los parámetros aquí ingresados.

Para especificar la configuración del servidor proxy en esta etapa, encienda el interruptor **Usar servidor proxy** y luego ingrese la dirección del servidor proxy en el campo **Servidor proxy**, junto con el número de **Puerto** del servidor proxy.

Si la comunicación con el servidor proxy requiere autenticación, encienda el interruptor **El servidor proxy requiere autenticación** e ingrese un **Nombre de usuario** y una **Contraseña** válidos en los campos respectivos. Haga clic en **Detectar** para detectar y llenar la configuración del servidor proxy en forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA

esta característica no recupera los datos de autenticación (nombre de usuario y contraseña); usted debe ingresarlos.

La configuración del servidor proxy también se puede establecer en la configuración de actualización avanzada (**Configuración avanzada > Actualizar > Proxy HTTP** seleccionando **Conexión mediante un servidor proxy** en el menú desplegable **Modo de proxy**). Esta configuración se aplica al perfil de actualización determinado y es recomendado para equipos portátiles, ya que suelen recibir las actualizaciones de firmas de virus desde distintas ubicaciones. Para obtener más información sobre esta configuración, consulte la sección [Configuración avanzada de la actualización](#).

4.6.8 Notificaciones por correo electrónico

ESET Mail Security puede enviar automáticamente correos electrónicos de notificación si ocurre un suceso con el nivel de detalle de los sucesos seleccionado. Habilite **Enviar notificaciones de sucesos por correo electrónico** para activar las notificaciones por correo electrónico.

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO 1

HERRAMIENTAS

Archivos de registro

Servidor proxy

Notificaciones por correo electrónico 1

Modo de presentación

Diagnósticos

Clúster

INTERFAZ DEL USUARIO

NOTIFICACIONES POR CORREO ELECTRÓNICO

Enviar notificaciones de sucesos por correo electrónico ☒

SERVIDOR SMTP

Servidor SMTP

Nombre de usuario

Contraseña

Dirección del remitente

Dirección del destinatario

Nivel de detalle mínimo para las notificaciones

Advertencias

Habilitar TLS ☐

Intervalo luego del cual se enviarán correos electrónicos de

Predeterminado

Aceptar

Cancelar

NOTA

Los servidores SMTP con cifrado TLS son admitidos por ESET Mail Security.

- **Servidor SMTP** : el servidor SMTP que se usa para enviar notificaciones.
- **Nombre de usuario y contraseña** : si el servidor SMTP requiere autenticación, se deben completar estos campos con un nombre de usuario y una contraseña válidos para acceder al servidor SMTP.
- **Dirección del remitente**: ingrese la dirección del remitente que aparecerá en el encabezado de los correos electrónicos de notificación. Esto es lo que el destinatario verá como **Desde**.
- **Dirección del destinatario** : especifique la dirección de correo electrónico del destinatario **Para** aquel al que se le enviarán notificaciones.
- **Nivel de detalle mínimo para las notificaciones**: especifica el nivel mínimo de detalle de las notificaciones que se enviarán.
- **Habilitar TLS**: habilita los mensajes de alertas y notificaciones admitidos por el cifrado TLS.
- **Intervalo luego del cual se enviarán correos electrónicos de notificación nuevos (min.)**: intervalo en minutos luego del cual se enviarán notificaciones nuevas mediante correo electrónico. Establezca el valor en 0 si desea enviar esas notificaciones inmediatamente.
- **Enviar cada notificación en un correo electrónico por separado**: cuando se habilite, el destinatario recibirá un correo electrónico nuevo por cada notificación individual. Esto puede dar como resultado un gran número de correos electrónicos recibidos en un corto periodo de tiempo.

Formato de mensajes

- **Formato de mensajes de sucesos** : formato de los mensajes de sucesos que se muestran en los equipos remotos. También consulte [Editar formato](#).
- **Formato de mensajes de advertencias sobre amenazas** : los mensajes de alerta y notificación de amenazas tienen un formato predeterminado predefinido. No es recomendable modificar dicho formato. No obstante, en ciertas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que necesite modificar el formato de los mensajes. También consulte [Editar formato](#).
- **Usar caracteres del alfabeto local** : convierte un mensaje de correo electrónico en la codificación de caracteres ANSI que se basa en la configuración de Windows Regional (por ejemplo, windows-1250). Si deja esta opción sin seleccionar, se convertirá y codificará un mensaje en ACSII de 7 bits (por ejemplo, “á” cambiará a “a” y un símbolo desconocido a “?”).
- **Usar la codificación local de caracteres** : el origen del mensaje de correo electrónico se codificará en el formato Entrecomillado imprimible (QP) que usa los caracteres de ASCII y puede transmitir correctamente los caracteres nacionales especiales por correo electrónico en el formato de 8 bits (áéíóú).

4.6.8.1 Formato de mensajes

Las comunicaciones entre el programa y el usuario remoto o el administrador del sistema se llevan a cabo por medio de los correos electrónicos o los mensajes de la LAN (mediante el servicio de mensajería de Windows®). El formato predeterminado de las notificaciones y los mensajes de alerta será óptimo para la mayoría de las situaciones. En ciertas circunstancias, es posible que necesite cambiar el formato de los mensajes de sucesos.

Las palabras clave (cadenas separadas por signos %) se reemplazan en el mensaje por la información real especificada. Se encuentran disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y la hora del suceso
- **%Scanner%**: módulo pertinente
- **%ComputerName%**: nombre del equipo en el que se produjo la alerta
- **%ProgramName%**: programa que generó la alerta
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado
- **%VirusName%**: identificación de la infección
- **%ErrorDescription%**: descripción de un suceso no causado por un virus

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se usan en mensajes de alerta de amenazas, y **%ErrorDescription%** solo se usa en mensajes de sucesos.

4.6.9 Modo presentación

El modo de presentación es una característica para los usuarios que requieren usar el software en forma ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. El modo de presentación también se puede usar durante las presentaciones que la actividad del programa antivirus no puede interrumpir. Cuando está habilitado, todas las ventanas emergentes se deshabilitan y las tareas programadas no se ejecutan. La protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

Haga clic en **Configuración > Equipo** y luego en el interruptor junto al **Modo presentación** para habilitar el modo de presentación en forma manual. En **Configuración avanzada (F5)**, haga clic en **Herramientas > Modo de presentación**; luego, haga clic en el interruptor junto a **Habilitar el modo de presentación automáticamente al ejecutar aplicaciones en modo de pantalla completa** para que ESET Mail Security active en forma automática el modo de presentación cuando se ejecutan las aplicaciones de pantalla completa. Habilitar el modo de presentación constituye un riesgo potencial para la seguridad; por ese motivo, el ícono de estado de protección ubicado en la barra de tareas se pondrá naranja y mostrará una advertencia. Esta advertencia también aparecerá en la ventana principal del programa, donde el **Modo de presentación habilitado** aparecerá en naranja.

Cuando **Habilitar el modo de presentación automáticamente al ejecutar aplicaciones de pantalla completa** está activo, el modo de presentación se iniciará siempre que abra una aplicación de pantalla completa y se detendrá automáticamente después de que salga de la aplicación. Es útil, en especial, para iniciar el modo de presentación inmediatamente luego de empezar un juego, abrir una aplicación de pantalla completa o iniciar una presentación.

También puede seleccionar **Deshabilitar el modo de presentación automáticamente después de** para definir la

cantidad de tiempo en minutos después de la que el modo de presentación se deshabilitará automáticamente.

4.6.10 Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET en caso de que se bloquee una aplicación (por ejemplo, *ekrn*). Si una aplicación se bloquea, se generará un volcado de memoria. Esto puede ayudar a los desarrolladores a depurar y reparar diversos problemas de ESET Mail Security. Haga clic en el menú desplegable junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Deshabilitar** (predeterminado) para deshabilitar esta característica.
- **Mini**: registra el grupo de datos útiles más reducido posible que pueda ayudar a identificar por qué se bloqueó la aplicación en forma inesperada. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, debido a la cantidad limitada de información incluida, es posible que los errores que no se provocaron directamente por el subprocesso activo en el momento del problema no se descubran al analizar este archivo.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene inesperadamente. Un volcado completo de memoria puede incluir datos de los procesos que estaban activos cuando se recopiló la memoria de volcado.

Habilitar el registro avanzado del filtrado de protocolos: registra todos los datos que pasan a través del motor de filtrado de protocolos para ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el filtrado de protocolos.

Directorio de destino: ubicación donde se va a generar la volcado de memoria durante el bloqueo.

Abrir carpeta de diagnósticos: haga clic en **Abrir** para abrir este directorio dentro de una nueva ventana del *Explorador de Windows*.

4.6.11 Atención al cliente

Enviar datos de configuración del sistema: seleccione **Enviar siempre** en el menú desplegable, o seleccione **Preguntar antes de enviar** para que se le solicite su autorización antes de enviar los datos.

4.6.12 Cluster

La opción **Habilitar clúster** se habilita de forma automática al configurar el clúster de ESET. Es posible deshabilitarlo de forma manual en la ventana de configuración avanzada, con un clic en el ícono del interruptor (es apropiado cuando se necesita cambiar la configuración sin afectar a otros nodos dentro del clúster de ESET). Este interruptor solo habilita o deshabilita la funcionalidad del clúster de ESET. Para configurar o eliminar el clúster de forma adecuada, es necesario usar el [Asistente de clúster](#) o “Destruir clúster”, opción que se encuentra en la sección **Herramientas > clúster** en la ventana principal del programa.

clúster de ESET no configurado y deshabilitado:

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO1

HERRAMIENTAS

Archivos de registro

Servidor proxy

Notificaciones por correo electrónico1

Modo de presentación

Diagnósticos

Clúster

INTERFAZ DEL USUARIO

CLÚSTER

Las configuraciones anteriores son habilitadas solamente cuando el clúster está activo.

Abrir puerto en el firewall de Windows

Intervalo de actualización del estado [seg.]

10

Sincronizar configuración del producto

INFORMACIÓN DE CONFIGURACIÓN

Las configuraciones anteriores solo pueden ser modificadas por el asistente del clúster.

Nombre de clúster

Puerto de escucha

9777

Lista de nodos de clúster

Predeterminado

Aceptar

Cancelar

clúster de ESET configurado adecuadamente con sus detalles y opciones:

Advanced setup

SERVER

COMPUTER

UPDATE

WEB AND EMAIL

DEVICE CONTROL

TOOLS

Log files

Proxy server

Email notifications

Presentation mode

Diagnostics

Cluster

USER INTERFACE

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ☒

Status refresh interval [sec]

Synchronize product settings ☒

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name termix

Listening port 9777

List of cluster nodes W2012R2-NODE1;W2012R2-NODE2;W2012R2-NODE3;WIN-JDLB8CEUR5

Default OK Cancel

Para mayor información sobre clústeres de ESET, haga clic [aquí](#).

4.7 Interfaz del usuario

La sección **Interfaz del usuario** permite configurar la conducta de la interfaz gráfica del usuario (GUI) del programa. Es posible ajustar el aspecto visual del programa y los efectos.

Para brindar la máxima seguridad de su software de seguridad, puede evitar los cambios no autorizados mediante la herramienta [Configuración de acceso](#).

En la configuración de las [Alertas y notificaciones](#), puede cambiar el comportamiento de las alertas sobre las amenazas detectadas y las notificaciones del sistema. Dichos mensajes se pueden personalizar acorde a sus necesidades.

Si elige no mostrar algunas notificaciones, aparecerán en el área [Mensajes y estados deshabilitados](#). Aquí puede verificar su estado, ver más detalles o quitarlas de esta ventana.

La [Integración en el menú contextual](#) aparece cuando se hace un clic con el botón secundario en un objeto seleccionado. Use esta herramienta para integrar los elementos de control de ESET Mail Security al menú contextual.

El [Modo presentación](#) es útil para los usuarios que deseen trabajar con una aplicación sin interrupciones de las ventanas emergentes, las tareas programadas o cualquier componente que pueda estresar los recursos del sistema.

Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz del usuario en ESET Mail Security permiten ajustar el entorno de trabajo conforme a sus necesidades. Puede acceder a estas opciones de configuración en la sección **Interfaz del usuario > Elementos de la interfaz del usuario** en el árbol de Configuración avanzada de ESET Mail Security.

En la sección **Elementos de la interfaz del usuario**, puede ajustar el entorno de trabajo. La interfaz del usuario debe

estar configurada en **Terminal** si los elementos gráficos ralentizan el rendimiento de su equipo o causan otros problemas. También es posible que desee deshabilitar la interfaz gráfica del usuario en un servidor Terminal. Para obtener más información acerca de ESET Mail Security instalado en un servidor Terminal, consulte el tema [Desactivar interfaz gráfica del usuario en servidor Terminal](#).

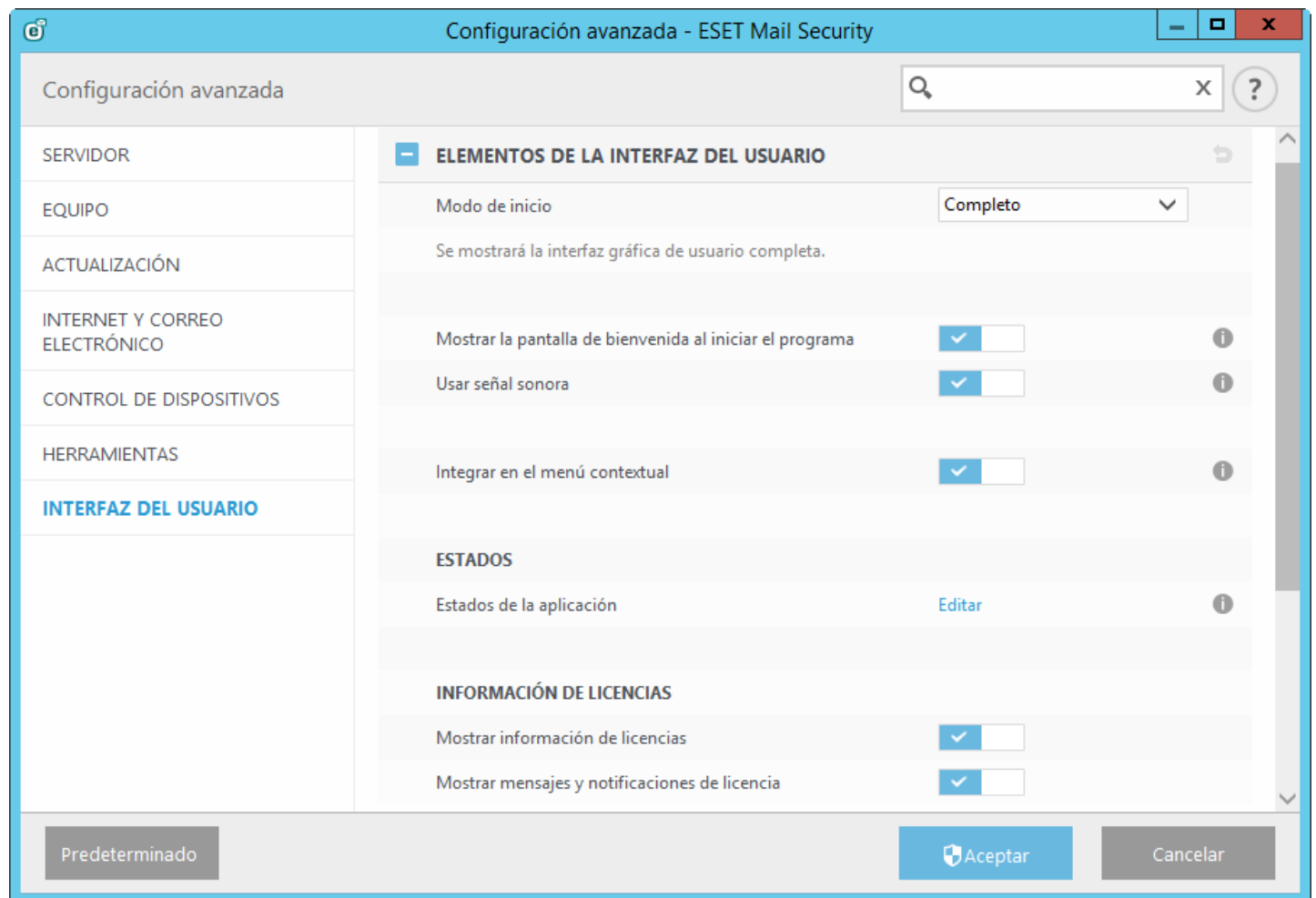
Haga clic en el menú desplegable del **Modo inicio** para seleccionar entre los siguientes Modos de inicio:

- **Completo**: se mostrará la GUI completa.
- **Terminal**: no se mostrará notificación o alerta alguna. La interfaz gráfica del usuario solo puede iniciarla el Administrador.

Si desea desactivar la pantalla de bienvenida de ESET Mail Security, quite la selección **Mostrar la pantalla de bienvenida al iniciar el programa**.

Para que ESET Mail Security reproduzca un sonido cuando ocurren sucesos importantes durante una exploración; por ejemplo, cuando se descubre una amenaza o cuando finaliza la exploración, seleccione **Usar señal sonora**.

Integrar en el menú contextual: integre los elementos de control de ESET Mail Security al menú contextual.



Estados: haga clic en [Editar](#) para administrar (habilitar o deshabilitar) los estados que se muestran en el panel [Supervisión](#) en el menú principal. **Estados de aplicaciones**: le permite habilitar o deshabilitar el estado de visualización en el panel **Estado de protección** en el menú principal.

Información de licencia : habilite esta opción. La información de licencia, los mensajes y las notificaciones habilitan esta opción.

4.7.1 Alertas y notificaciones

La sección **Alertas y notificaciones** en **Interfaz del usuario** permite configurar la forma en que ESET Mail Security gestionará las alertas ante las amenazas y las notificaciones del sistema (p. ej., los mensajes sobre las actualizaciones correctas). También puede establecer el tiempo de visualización y la transparencia de las notificaciones en la bandeja del sistema (esto solo se aplica en los sistemas que son compatibles con las notificaciones en la bandeja del sistema).

Ventanas de alerta

Si deshabilita **Mostrar alertas**, se cancelarán todas las ventanas de alerta, lo que es apropiado únicamente para una cantidad limitada de situaciones específicas. Para la mayoría de los usuarios, recomendamos dejar esta opción en su configuración predeterminada (es decir, habilitada).

Notificaciones en el escritorio

Las notificaciones en el escritorio y los globos de sugerencias son solo informativos y no necesitan la interacción con el usuario. Se muestran en el área de notificaciones en la esquina inferior derecha de la pantalla. Para activar las notificaciones en el escritorio, seleccione la opción **Mostrar notificaciones en el escritorio**. A continuación, se pueden modificar las opciones más detalladas, como el tiempo de visualización de las notificaciones y la transparencia de la ventana.

Encienda el interruptor **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones no interactivas.

Configuración avanzada

SERVIDOR

EQUIPO

ACTUALIZACIÓN

INTERNET Y CORREO ELECTRÓNICO

CONTROL DEL DISPOSITIVO 1

HERRAMIENTAS 1

INTERFAZ DEL USUARIO

ALERTAS Y NOTIFICACIONES

VENTANAS DE ALERTA

Mostrar alertas ☒

NOTIFICACIONES EN EL ESCRITORIO

Mostrar notificaciones en el escritorio ☒

No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa ☒

Duración 10

Transparencia 20

Cantidad mínima de detalle de sucesos para mostrar Informativo

En sistemas con varios usuarios, mostrar notificaciones en la pantalla del siguiente usuario Administrator

CUADROS DE MENSAJES

Cerrar cuadros de mensajes automáticamente ☒

Predeterminado Aceptar Cancelar

El menú desplegable **Cantidad mínima de detalle de sucesos para mostrar** le permite seleccionar el nivel de gravedad de las alertas y notificaciones que se mostrarán. Se encuentran disponibles las siguientes opciones:

- **Diagnóstico:** registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo:** registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias:** registra los errores críticos y los mensajes de advertencia.
- **Errores:** se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico:** registra solo los errores críticos (error al iniciar la protección antivirus, etc.).

La última característica de esta sección permite configurar el destino de las notificaciones en un entorno con varios usuarios. El campo **En sistemas con varios usuarios, mostrar notificaciones en la pantalla de este usuario** especifica qué usuario recibirá las notificaciones del sistema y otros tipos de notificaciones en los sistemas que permiten que se conecten varios usuarios al mismo tiempo. Normalmente, se trata de un administrador del sistema o de la red. Esta opción resulta especialmente útil para los servidores de terminal, siempre y cuando todas las notificaciones del sistema se envíen al administrador.

Cuadros de mensajes

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione **Cerrar las casillas de mensajes automáticamente**. Si no se cierran manualmente, las ventanas de alerta se cerrarán en forma automática una vez que transcurra el período especificado.

4.7.2 Configuración del acceso

Para proporcionarle a su sistema la máxima seguridad, es esencial que ESET Mail Security esté configurado correctamente. Cualquier cambio no calificado puede provocar la pérdida de datos importantes. Para evitar las modificaciones no autorizadas, puede proteger los parámetros de configuración de ESET Mail Security con una contraseña. Las propiedades de la configuración para la protección con contraseña se encuentran en el submenú **Configuración del acceso** bajo **Interfaz del usuario** en el árbol de configuración avanzada.

Configuración avanzada

x
?

SERVIDOR	+ ELEMENTOS DE LA INTERFAZ DEL USUARIO
EQUIPO	+ ALERTAS Y NOTIFICACIONES
ACTUALIZACIÓN	- CONFIGURACIÓN DEL ACCESO
INTERNET Y CORREO ELECTRÓNICO	Configuración de la protección por contraseña x
CONTROL DEL DISPOSITIVO 1	Establecer contraseña Establecer
HERRAMIENTAS 1	Exigir derechos completos de administrador para cuentas de administrador limitadas <input checked="" type="checkbox"/>
INTERFAZ DEL USUARIO	+ AYUDA
	+ SHELL DE ESET

Predeterminado

Aceptar

Cancelar

Configuración de la protección por contraseña: bloquea o desbloquea los parámetros de configuración del programa. Haga clic para abrir la ventana de Configuración de la contraseña.

Si desea establecer o modificar una contraseña para proteger los parámetros de configuración, haga clic en

Establecer contraseña.

Exigir derechos completos de administrador para cuentas de administrador limitadas: seleccione esta opción para solicitarle al usuario actual (si no dispone de derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador cuando modifique determinados parámetros del sistema (similar a UAC en Windows Vista). Las modificaciones incluyen la deshabilitación de los módulos de protección.

4.7.2.1 Contraseña

Para evitar la modificación no autorizada, los parámetros de configuración de ESET Mail Security pueden protegerse con una contraseña.

4.7.2.2 Configuración de la contraseña

Para proteger los parámetros de configuración de ESET Mail Security y evitar una modificación no autorizada, debe establecer una contraseña nueva. Cuando desee cambiar una contraseña existente, escriba su contraseña anterior en el campo **Contraseña anterior**, ingrese su nueva contraseña en los campos **Contraseña nueva** y **Confirmar contraseña** y luego, haga clic en **Aceptar**. Esta contraseña será necesaria para futuras modificaciones de ESET Mail Security.

4.7.3 Ayuda

Cuando presiona la tecla **F1** o hace clic en el botón **?**, se abre una ventana de ayuda en línea. Esta es la fuente principal de contenido de ayuda. Sin embargo, también hay una copia de ayuda fuera de línea que viene instalada con el programa. La ayuda fuera de línea se abre en casos tales como cuando no hay conexión a Internet.

La última versión de la Ayuda en línea se muestra de forma automática cuando tiene una conexión a Internet.

4.7.4 Shell de ESET

Puede configurar los derechos de acceso para la configuración del producto, las características y los datos a través de eShell al cambiar la **Política de ejecución del Shell de ESET**. La configuración predeterminada es **Cifrado limitado**, pero puede cambiarla a **Deshabilitado**, **Solo lectura** o **Acceso completo** de ser necesario.

- **Deshabilitado:** eShell no puede usarse en lo absoluto. Solo se permite la configuración de eShell en el contexto de la interfaz del usuario de eShell. Puede personalizar la apariencia de eShell, pero no puede acceder a las configuraciones ni a los datos de ningún producto.
- **Solo lectura:** eShell se puede usar como una herramienta de monitoreo. Puede visualizar todas las configuraciones tanto en el modo interactivo como en el de procesamiento por lotes, pero no puede modificar las configuraciones, las funciones ni los datos.
- **Cifrado limitado:** en modo interactivo, puede visualizar y modificar todas las configuraciones, las funciones y los datos. En el modo de Lote, eShell funcionará como si estuviera en modo de solo lectura, no obstante, si usa archivos de lotes firmados, podrá editar las configuraciones y modificar los datos.
- **Acceso completo:** el acceso a todas las configuraciones es ilimitado tanto en modo interactivo como de procesamiento por lotes (al ejecutar archivos por lotes). Puede visualizar y modificar cualquier configuración. Debe usar una cuenta de administrador para ejecutar eShell con acceso completo. Si UAC está habilitado, también se requiere elevación.

4.7.5 Deshabilitación de la interfaz gráfica del usuario en Terminal Server

Este capítulo describe cómo deshabilitar la interfaz gráfica del usuario de ESET Mail Security cuando se ejecuta en Windows Terminal Server para sesiones de usuario.

Normalmente, la interfaz gráfica del usuario de ESET Mail Security se inicia cada vez que un usuario remoto se registra en el servidor y crea una sesión de terminal. Por lo general, esto no es deseable en servidores Terminal Server. Si desea deshabilitar la interfaz gráfica del usuario para sesiones terminales, puede hacerlo mediante [eShell](#) al ejecutar `configurar` el comando `ui ui gui-start-mode terminal`. Esto pondrá la interfaz gráfica del usuario en modo terminal. Estos son los dos modos disponibles para el inicio de la interfaz gráfica del usuario:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Si desea averiguar qué modo se usa actualmente, ejecute el comando `get ui ui gui-start-mode`.

NOTA

en caso de que tenga instalado ESET Mail Security en un servidor con Citrix, le recomendamos usar las configuraciones descritas en nuestro [artículo KB](#).

4.7.6 Mensajes y estados deshabilitados

Mensajes de confirmación: le muestra una lista de mensajes de confirmación que puede seleccionar para que se muestren o no.

Estados de aplicaciones deshabilitados: le permite habilitar o deshabilitar la visualización del estado en el panel **Estado de protección** en el menú principal.


4.7.6.1 Mensajes de confirmación

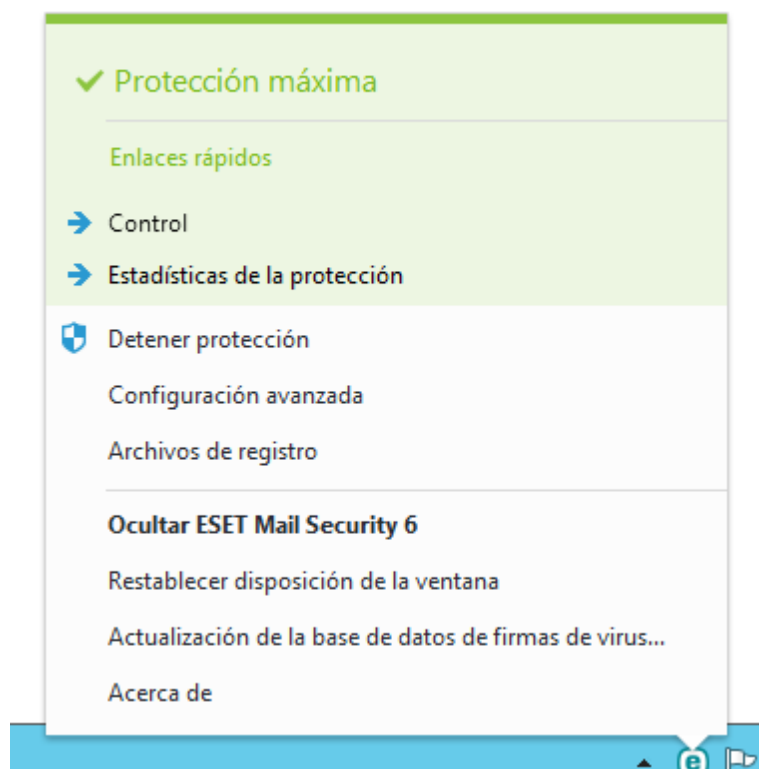
Esta ventana de diálogo muestra los mensajes de confirmación que mostrará ESET Mail Security antes de que se realice alguna acción. Seleccione o anule la selección de la casilla de verificación junto a cada mensaje de confirmación para permitirlo o deshabilitarlo.

4.7.6.2 Estados de aplicaciones deshabilitados

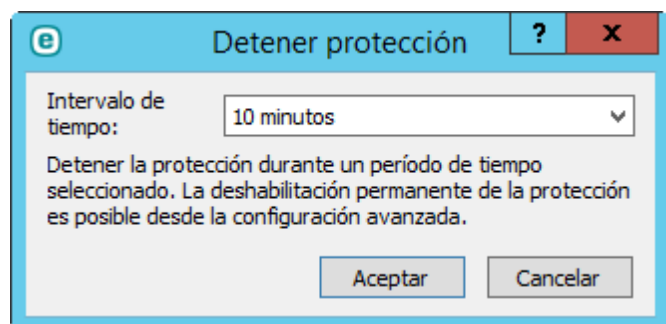
En esta ventana de diálogo, puede seleccionar o anular la selección de los estados de las aplicaciones que se mostrarán o no. Por ejemplo, cuando detiene la protección antivirus y antispyware, o cuando habilita el modo de presentación. Un estado de aplicaciones también se mostrará si su producto no está activado o si su licencia ha vencido.

4.7.7 Ícono de la bandeja del sistema

Algunas de las opciones de configuración y funciones más importantes están disponibles al hacer clic con el botón secundario en el ícono de la bandeja del sistema .



Detener la protección: muestra el cuadro de diálogo de confirmación que deshabilita la [Protección antivirus y antispyware](#), que protege ante ataques mediante el control de los archivos, las comunicaciones por medio de Internet y correo electrónico.



El menú desplegable **Intervalo de tiempo** representa el período durante el cual la protección antivirus y antispyware permanecerá deshabilitada.

Configuración avanzada: seleccione esta opción para ingresar en el árbol de **Configuración avanzada**. También puede acceder a la Configuración avanzada al presionar la tecla F5 o al ir a **Configuración > Configuración avanzada**.

Archivos de registro: los [archivos de registro](#) contienen información sobre todos los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas.

Ocultar ESET Mail Security: se oculta la ventana ESET Mail Security de la pantalla.


Restablecer la disposición de la ventana: restablece la ventana de ESET Mail Security a su tamaño y posición predeterminados en la pantalla.

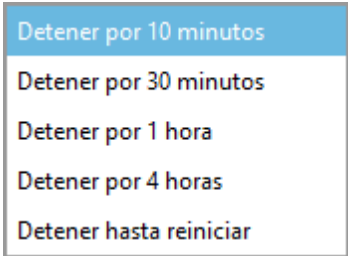
Actualización de la base de datos de firmas de virus: comienza a actualizar la base de datos de firmas de virus para garantizar su nivel de protección frente a un código malicioso.

Acerca de: proporciona información del sistema, detalles sobre la versión instalada de ESET Mail Security y los módulos del programa instalados, como así también la fecha de vencimiento de su licencia. La información acerca de

su sistema operativo y recursos del sistema se puede encontrar en la parte inferior de la página.

4.7.7.1 Detener protección

Cada vez que hace una pausa temporal en el signo de protección antivirus y antispymware en el icono de la bandeja del sistema , aparece el cuadro de diálogo **Pausa temporal de la protección**. Esto deshabilita la protección relacionada con el malware durante el periodo de tiempo seleccionado (para deshabilitar la protección permanentemente, debe usar la Configuración avanzada). Tenga precaución, deshabilitar la protección puede exponer su equipo a amenazas.

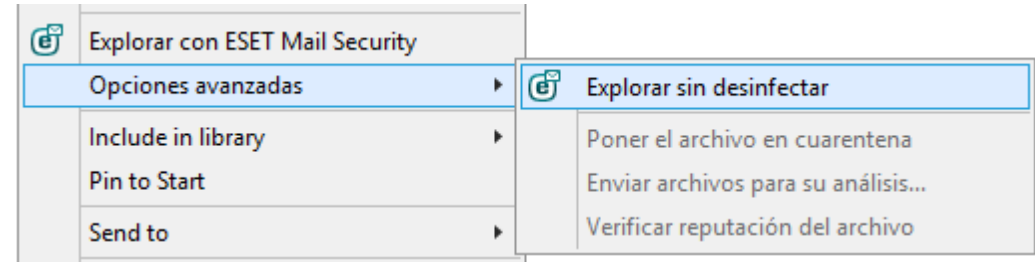


4.7.8 Menú contextual

El menú contextual aparece cuando se hace un clic con el botón secundario en un objeto (archivo). El menú muestra una lista de todas las acciones que puede realizar en un objeto.

Es posible integrar los elementos de control de ESET Mail Security al menú contextual. Las opciones de configuración para esta función están disponibles en el árbol de Configuración avanzada, en **Interfaz del usuario > Elementos de la interfaz del usuario**.


Integrar en el menú contextual: integre los elementos de control de ESET Mail Security al menú contextual.



4.8 Revertir toda la configuración en esta sección

Restaura las configuraciones de los módulos a las configuraciones predeterminadas definidas por ESET. Tenga en cuenta que cualquier cambio que se haya hecho, se perderá después de hacer clic en **Restaurar a predeterminado**.

Restaurar el contenido de las tablas: cuando se habilitan, las reglas, las tareas o los perfiles que se hayan agregado de manera manual o automática se perderán.

Revertir a la configuración predeterminada 

¿Revertir toda la configuración en esta sección?

Esto revertirá la configuración a los valores predeterminados y cualquier cambio realizado luego de la instalación se perderá. Esta acción no se puede deshacer.


Revertir los contenidos de las tablas ☐

Cualquier dato agregado a las tablas y las listas (por ej. reglas, tareas, perfiles) ya sea manual o automáticamente se perderá

Revertir a predeterminado Cancelar

4.9 Revertir a la configuración predeterminada

Todas las configuraciones del programa, para todos los módulos, se restablecerán al estado que tendrían después de su instalación inicial.

Revertir a la configuración predeterminada 

¿Revertir toda la configuración?

Esto revertirá la configuración a los valores predeterminados y cualquier cambio realizado luego de la instalación se perderá. Esta acción no se puede deshacer.

Revertir a predeterminado Cancelar

4.10 Programador

Podrá encontrar el **Tareas programadas** en la sección **Herramientas** de la ventana del programa principal. En las tareas programadas se administran y se ejecutan tareas programadas, según los parámetros definidos.

Tareas programadas enumera todas las tareas programadas en forma de tabla y muestra sus parámetros, como tipo de **Tarea**, **Nombre de la tarea**, **Hora de ejecución** y **Última ejecución**. Para obtener más información, haga doble clic sobre una tarea para ver el [Resumen general de tareas programadas](#). Después de la instalación, hay un conjunto de tareas predefinidas. También puede crear nuevas tareas programadas si hace clic en [Agregar tarea](#).

Cuando hace clic con el botón secundario sobre una tarea, puede elegir la acción que desea realizar. Las acciones disponibles son:

Mostrar detalles de la tarea

Ejecutar ahora

Agregar...

Editar...

Eliminar

Use la casilla de verificación junto a la tarea para activarla/desactivarla. Para editar la configuración de una tarea programada, haga un clic con el botón secundario en la tarea y luego en **Editar...** o seleccione la tarea que quiera modificar y haga clic en **Editar**.

Tarea	Nombre	Hora de inicio	Última ejecución
<input checked="" type="checkbox"/> Mantenimiento de reg...	Mantenimiento de registros	La tarea se ejecutará todo...	25-Aug-15 3:35:05 PM
<input checked="" type="checkbox"/> Actualización	Actualización automática ...	La tarea se ejecutará reiter...	25-Aug-15 4:35:06 PM
<input checked="" type="checkbox"/> Actualización	Actualización automática ...	Conexión por módem a In...	
<input type="checkbox"/> Actualización	Actualización automática ...	El usuario inicie la sesión (...)	
<input checked="" type="checkbox"/> Verificación de archiv...	Verificación de archivos d...	El usuario inicie la sesión ...	25-Aug-15 3:37:36 PM
<input checked="" type="checkbox"/> Verificación de archiv...	Verificación de archivos d...	Se haya actualizado corre...	25-Aug-15 4:35:29 PM
<input checked="" type="checkbox"/> Primera exploración	Primera exploración auto...	La tarea se ejecutará una s...	25-Aug-15 3:54:06 PM

Las tareas programadas predeterminadas (predefinidas) son:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática después de la conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**
- **Exploración automática de archivos durante el inicio del sistema** (después del registro del usuario)
- **Exploración automática de archivos durante el inicio del sistema** (tras la actualización correcta de la base de datos de firmas de virus)
- **Primera exploración automática**

4.10.1 Detalles de tarea

Ingrese el **Nombre de la tarea** y seleccione el **Tipo de tarea** que desee del menú desplegable:

- **Ejecutar aplicación externa:** programa la ejecución de una aplicación externa.
- **Mantenimiento de registros:** los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema:** verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo:** crea una instantánea del equipo de [<%ESI%>](#), que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a petición:** realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Primera exploración:** de manera predeterminada, 20 minutos después de la instalación o reinicio se realizará una exploración del equipo como una tarea de prioridad baja.
- **Actualizar:** programa una tarea de actualización mediante la actualización de la base de datos de firmas de virus y los módulos del programa.
- **Exploración de la base de datos:** le permite programar una exploración de la base de datos y elegir elementos para ser explorados. Básicamente, es una [Exploración de la base de datos a petición](#).

NOTA

Si usted tiene la [protección de base de datos de la casilla de correo](#) habilitada, todavía puede programar esta tarea, pero finalizará con un mensaje de error que se mostrará en la sección [Exploración](#) de la GUI principal que dice **Exploración de la base de datos - Exploración interrumpida debido a un error**. Para evitar esto, debe asegurarse de que la protección de la base de datos de la casilla de correo esté deshabilitada durante el horario en que la **Exploración de la base de datos** se programó para su ejecución.

- **Enviar informes de cuarentena de correo:** programa un [Informe de cuarentena de correo para enviarse por correo electrónico](#).
- **Exploración en segundo plano:** le da la oportunidad al servidor Exchange Server de [ejecutar una exploración de la base de datos en segundo plano](#) de ser necesario.

Si desea desactivar la tarea después de crearla, haga clic en el interruptor junto a **Habilitado**. Podrá activar la tarea más tarde mediante la casilla de verificación en la vista [Tareas programadas](#).

Haga clic en el botón **Siguiente** para continuar al [siguiente paso](#).

4.10.2 Programación de tareas: única vez

Especifique la fecha y la hora de la **Ejecución de tareas** por única vez.

4.10.3 Programación de tarea

Seleccione una de las opciones de programación cuando desee **ejecutar la tarea programada**:

- **Una vez:** la tarea se realizará solo una vez en una fecha y hora específica.
- **Reiteradamente:** la tarea se realizará con el intervalo de tiempo especificado (en minutos).
- **Diariamente:** la tarea se ejecutará reiteradamente todos los días a la hora especificada.
- **Semanalmente:** la tarea se ejecutará una o varias veces a la semana, en los días y a la hora especificados.
- **Cuando se cumpla la condición:** la tarea se ejecutará luego de un suceso especificado.

Omitir tarea al ejecutar con alimentación de la batería: la tarea no se ejecutará si el sistema funciona con baterías en el momento en que la tarea debería iniciarse. Se aplica a equipos que reciben alimentación de un SAI, por ejemplo.

Haga clic en el botón **Siguiente** para continuar al siguiente paso.

4.10.4 Programación de tareas: a diario

Especifique la hora en que se ejecutará la tarea todos los días.

4.10.5 Programación de tareas: semanalmente

La tarea se ejecutará el día y a la hora especificados.

4.10.6 Programación de tareas: accionada por suceso

La tarea se puede accionar por uno de los siguientes sucesos:

- **Cada vez que se inicie el equipo**
- **La primera vez que se inicie el equipo en el día**
- **conexión por módem a Internet/VPN**
- **Actualización correcta de la base de datos de firmas de virus**
- **Actualización correcta de los componentes del programa**
- **Inicio de sesión del usuario**
- **Detección de amenazas**

Cuando se programa una tarea accionada por un suceso, puede especificar el intervalo mínimo entre dos ejecuciones completas de la tarea. Por ejemplo, si inicia la sesión en su equipo varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, posteriormente, al día siguiente.

4.10.7 Detalles de la tarea: lanzar la aplicación

Esta tarea programa la ejecución de una aplicación externa.

- **Archivo ejecutable:** elija un archivo ejecutable desde el árbol del directorio, haga clic en la opción ... e ingrese la ruta en forma manual.
- **Carpeta de trabajo:** defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **Archivo ejecutable** seleccionado se crearán dentro de este directorio.
- **Parámetros:** parámetros de la línea de comandos de la aplicación (opcional).

Haga clic en **Terminar** para crear la tarea o aplicar los cambios, si modificó la tarea programada existente.

4.10.8 Detalles de la tarea: enviar informes de cuarentena de correo

Esta tarea programa un informe de Cuarentena de correo que se envía por correo electrónico.

- **Dirección del remitente:** especifica una dirección de correo electrónico que se mostrará como remitente del informe de cuarentena de correo.
- **Cuenta máx. de registros en el informe:** puede limitar la cantidad de entradas en un informe. El recuento predeterminado es 50.
- **URL web:** esta URL se incluirá en el informe de cuarentena de correo para que el destinatario pueda hacer clic simplemente para acceder a la interfaz web de la cuarentena de correo.
- **Destinatarios:** seleccione los usuarios que recibirán los informes de cuarentena de correo. Haga clic en **Editar** para seleccionar los buzones de correo para destinatarios específicos. Puede seleccionar múltiples destinatarios.

Haga clic en **Finalizar** para crear la tarea programada.

4.10.9 Pasar por alto tarea

Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se realizará:

- **A la próxima hora programada** : la tarea se ejecutará a la hora especificada (por ejemplo, luego de 24 horas).
- **Lo antes posible**: la tarea se ejecutará lo antes posible, cuando las acciones que impiden que se ejecute dejen de ser válidas.
- **Inmediatamente, si el tiempo desde la última ejecución excede un valor específico: Tiempo desde la última ejecución (horas)**: luego de seleccionar esta opción, la tarea se repetirá siempre al transcurrir el período especificado (en horas).

4.10.10 Resumen general de tareas programadas

Esta ventana de diálogo muestra información detallada sobre la tarea programada cuando hace doble clic en la tarea en la vista [Programador de tareas](#) o cuando hace clic con el botón secundario en la tarea programada y elige **Mostrar detalles de la tarea**.

Resumen general de tareas programadas

Nombre de tarea

Actualización automática de rutina

Tipo de tarea

Actualización

Ejecutar la tarea

La tarea se ejecutará reiteradamente cada cada 60 minutos.

Acción en caso de que la tarea no se ejecute en el momento especificado

A la siguiente hora programada

Aceptar

4.10.11 Tareas del programador: exploración en segundo plano

Exploración en segundo plano: este tipo de tarea permite la exploración de la base de datos mediante VSAPI en segundo plano. Básicamente permite que Exchange Server ejecute una exploración en segundo plano si es necesario. La exploración se inicia el mismo Exchange Server, esto significa que Exchange Server decide si la exploración se ejecutará dentro del tiempo permitido.

Le recomendamos que permita que esta tarea se ejecute fuera de las horas picos cuando Exchange Server no esté ocupado, por ejemplo durante la noche. Esto se debe a que la exploración en segundo plano de la base de datos coloca cierta cantidad de carga en el sistema. Además, el periodo de tiempo no debe entrar en conflicto con cualquier copia de seguridad que pueda estar ejecutándose en Exchange Server para evitar problemas de rendimiento o disponibilidad.

i NOTA

La [Protección de la base de datos del buzón de correo](#) debe estar habilitada para que se ejecute la tarea del programador. Este tipo de protección solamente está disponible para Microsoft Exchange Server 2010, 2007 y 2003 que funciona en rol de Servidor del buzón de correo (Microsoft Exchange 2010 y 2007) o Servidor back-end

Tiempo de espera (horas): especifica cuántas horas tiene permitido Exchange Server para ejecutar la exploración en segundo plano de la base de datos desde la hora en que se ejecuta la tarea programada. Una vez que alcanza el tiempo de espera, se le indicará a Exchange que detenga la exploración en segundo plano.

4.10.12 Perfiles de actualización

Si desea actualizar el programa desde dos servidores de actualización, será necesario crear dos perfiles de actualización diferentes. Si el primero no logra descargar los archivos de actualización, el programa cambia automáticamente al perfil alternativo. Esto es conveniente, por ejemplo, para equipos portátiles, que suelen actualizarse desde un servidor de actualización de la red de área local, pero cuyos dueños normalmente se conectan a Internet por medio de otras redes. Por lo tanto, si falla el primer perfil, el segundo descargará automáticamente los archivos de actualización desde los servidores de actualización de ESET.

Puede obtener más información sobre los perfiles de actualización en el capítulo [Actualizar](#).

4.11 Cuarentena

[Envío de archivos a cuarentena](#)

ESET Mail Security pone automáticamente en cuarentena los archivos eliminados (si no ha deshabilitado esta opción en la ventana de alerta). Si lo desea, es posible enviar a cuarentena cualquier archivo sospechoso en forma manual mediante un clic en el botón **Cuarentena**. Los archivos en cuarentena se eliminarán de su ubicación original. También se puede usar el menú contextual con este propósito. Para ello, haga clic con el botón secundario en la ventana **Cuarentena** y seleccione **Cuarentena**.

[Restauración desde cuarentena](#)

Los archivos puestos en cuarentena también pueden restaurarse a su ubicación original. Para ello, use la función **Restaurar**, disponible desde el menú contextual tras hacer un clic con el botón secundario en el archivo determinado en la ventana Cuarentena. Si un archivo está marcado como una aplicación potencialmente no deseada, la opción **Restablecer y excluir de la exploración** estará disponible. Lea más información sobre este tipo de aplicación en el [glosario](#). Asimismo, el menú contextual ofrece la opción **Restaurar a...**, que permite restaurar un archivo en una ubicación diferente a la que tenía cuando fue eliminado.

NOTA

si el programa puso en cuarentena un archivo no infectado por error, [exclúyalo de la exploración](#) después de restaurarlo y envíelo a Atención al cliente de ESET.

[Envío de un archivo desde cuarentena](#)

Si puso en cuarentena un archivo sospechoso que el programa no detectó o si un archivo se determinó erróneamente como infectado (por ejemplo, tras la exploración heurística del código) y luego se puso en cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivo desde la cuarentena, haga clic en el archivo con el botón secundario y seleccione **Enviar para su análisis** en el menú contextual.

4.11.1 Envío de archivos a cuarentena

ESET Mail Security pone automáticamente en cuarentena los archivos eliminados (si no ha deshabilitado esta opción en la ventana de alerta). Si lo desea, es posible enviar a cuarentena cualquier archivo sospechoso en forma manual mediante un clic en el botón **Cuarentena**. En este caso, el archivo original no se quita de su ubicación inicial. También se puede usar el menú contextual con este propósito. Para ello, haga clic con el botón secundario en la ventana **Cuarentena** y seleccione **Cuarentena**.

4.11.2 Restauración desde cuarentena

Los archivos puestos en cuarentena también pueden restaurarse a su ubicación original. Para restablecer un archivo en cuarentena, haga clic con el botón secundario en el mismo en la ventana Cuarentena, y seleccione **Restablecer** en el menú contextual. Si un archivo está marcado como una [aplicación potencialmente no deseada](#), **Restablecer y excluir de la exploración** también estará disponible. Asimismo, el menú contextual contiene la opción **Restablecer a...**, que le permite restablecer un archivo en una ubicación diferente a la que tenía cuando fue eliminado.

Eliminar de la Cuarentena: haga clic con el botón secundario en un elemento determinado y seleccione **Eliminar de la Cuarentena**, o seleccione el elemento que desea eliminar y presione **Eliminar** en su teclado. También puede seleccionar varios elementos y eliminarlos todos juntos.

NOTA

si el programa puso en cuarentena un archivo no infectado por error, [exclúyalo de la exploración](#) después de restaurarlo y envíelo a Atención al cliente de ESET.

4.11.3 Envío de archivos desde cuarentena

Si puso en cuarentena un archivo sospechoso que el programa no detectó o si un archivo fue catalogado erróneamente como infectado (por ejemplo, tras la exploración heurística del código) y luego se puso en cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivo desde la cuarentena, haga clic en el archivo con el botón secundario y seleccione **Enviar para su análisis** en el menú contextual.

4.12 Actualizaciones del sistema operativo

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El nivel de prioridad de la actualización aparece junto al nombre de la actualización.

Haga clic en **Ejecutar la actualización del sistema** para comenzar la descarga e instalación de las actualizaciones del sistema operativo.

Haga un clic con el botón secundario en cualquier línea de actualización y luego haga clic en **Mostrar información** para abrir una ventana emergente con información adicional.

5. Glosario

5.1 Tipos de infiltraciones

Una infiltración es un programa con códigos maliciosos que intenta ingresar al equipo del usuario y/o dañarlo.

5.1.1 Virus

Un virus informático es una infiltración que daña los archivos existentes en el equipo. Se denominaron así por los virus biológicos, ya que usan técnicas similares para propagarse desde un equipo a otro.

Los virus informáticos atacan principalmente a los archivos ejecutables y los documentos. Para replicarse, el virus adjunta su “cuerpo” al final del archivo de destino. En resumen, el virus informático funciona de esta forma: luego de la ejecución del archivo infectado, el virus se activa (antes de la aplicación original) y desempeña la tarea predefinida. Recién cuando termina de hacerlo, permite que se ejecute la aplicación original. Un virus no puede infectar un equipo a menos que un usuario, ya sea en forma accidental o deliberada, ejecute o abra el programa malicioso.

Los virus informáticos pueden variar en su objetivo y gravedad. Algunos son extremadamente peligrosos debido a su capacidad de eliminar archivos del disco duro en forma deliberada. Por otra parte, algunos virus no provocan ningún daño: solo sirven para molestar al usuario y demostrar las habilidades técnicas de sus creadores.

Es importante destacar que los virus (al compararlos con los troyanos o los spyware) cada vez son menos frecuentes, ya que los autores de programas maliciosos no los encuentran comercialmente atractivos. Además, el término “virus” se suele usar de manera incorrecta para abarcar todos los tipos de infiltraciones. El uso indebido del término se está superando gradualmente y se lo está reemplazando por el nuevo término, más apropiado, “malware” (programa malicioso).

Si su equipo está infectado con un virus, será necesario restaurar los archivos infectados a su estado original, es decir, desinfectarlos mediante un programa antivirus.

Algunos ejemplos de virus son: OneHalf, Tenga y Yankee Doodle.

5.1.2 Gusanos

Un gusano informático es un programa que contiene códigos maliciosos que atacan a los equipos host y se propagan a través de una red. La diferencia básica entre un virus y un gusano es que los gusanos tienen la capacidad de replicarse y viajar por sí mismos; no dependen de archivos host (o de sectores de inicio). Los gusanos se propagan por medio de mensajes de correo electrónico a la lista de contactos del usuario o aprovechan vulnerabilidades de seguridad en aplicaciones de red.

Como consecuencia, los gusanos son mucho más viables que los virus informáticos. Debido a la alta disponibilidad de Internet, pueden propagarse alrededor del mundo en cuestión de horas e incluso minutos desde su lanzamiento. Esta capacidad de replicarse en forma independiente y rápida los hace más peligrosos que otros tipos de malware.

Un gusano activado en un sistema puede provocar una serie de inconvenientes: eliminar archivos, afectar perjudicialmente el rendimiento del sistema o incluso desactivar programas. La naturaleza del gusano informático le permite servir de “medio de transporte” para otros tipos de infiltraciones.

Si su equipo está infectado con un gusano, se recomienda eliminar los archivos infectados, ya que probablemente contengan códigos maliciosos.

Algunos ejemplos de gusanos conocidos son: Lovsan/Blaster, Stration/Warezov, Bagle y Netsky.

5.1.3 Troyanos

Históricamente, los troyanos (o caballos de Troya) informáticos se definieron como una clase de infiltración que intenta pasar por un programa útil y engañar a los usuarios para que los dejen ejecutarse. Sin embargo, es importante aclarar que esto era cierto para los troyanos en el pasado; hoy en día, ya no tienen la necesidad de disfrazarse. Su único propósito es infiltrarse lo más fácilmente posible y cumplir sus objetivos maliciosos. “Troyano” se convirtió en un término muy general para describir cualquier infiltración que no entre en ninguna otra clasificación específica.

Como se trata de una categoría muy amplia, a menudo se divide en muchas subcategorías:

- **Descargador:** es un programa malicioso con capacidad de descargar otras infiltraciones desde Internet
- **Lanzador:** es un tipo de troyano diseñado para lanzar otros tipos de malware a equipos expuestos
- **Programa de puerta trasera:** es una aplicación que se comunica con atacantes remotos, lo que les permite obtener acceso a un sistema y controlarlo
- **Registrador de pulsaciones de teclas:** es un programa que registra cada pulsación que el usuario hace en el teclado y envía la información a atacantes remotos
- **Marcador:** es un programa diseñado para conectar el equipo a números con tarifas más elevadas de lo normal. Resulta casi imposible que el usuario advierta que se creó una nueva conexión. Los marcadores solo pueden perjudicar a los usuarios que se conectan a Internet a través de un módem de discado telefónico, lo que está dejando de ser habitual.

Los troyanos por lo general adoptan la forma de archivos ejecutables con extensión .exe. Si un archivo de su equipo se identifica como un troyano, se aconseja eliminarlo, ya que lo más probable es que contenga códigos maliciosos.

Algunos ejemplos de troyanos conocidos son: NetBus, Trojandownloader. Small.ZL, Slapper.

5.1.4 Rootkits

Los rootkits son programas maliciosos que les garantizan a los atacantes por Internet acceso ilimitado a un sistema, a la vez que ocultan su presencia. Los rootkits, luego de acceder al sistema (usualmente explotando la vulnerabilidad de un sistema), usan las funciones en el sistema operativo para evitar la detección del programa antivirus: ocultan procesos, archivos y datos del registro de Windows, etc. Por esta razón, es casi imposible detectarlos por medio de técnicas de evaluación comunes.

Existen dos niveles de detección para prevenir rootkits:

- 1) Cuando intentan acceder al sistema. Todavía no están presentes, por lo tanto están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (asumiendo que realmente detectan dichos archivos como infectados).
- 2) Cuando se ocultan de la evaluación común, los usuarios de ESET Mail Security tienen la ventaja de contar con la tecnología Anti-Stealth, que también puede detectar y eliminar rootkits activos.

5.1.5 Adware

Adware es el término abreviado correspondiente a un programa relacionado con la publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Las aplicaciones de adware suelen abrir automáticamente una nueva ventana emergente con avisos publicitarios en un navegador de Internet o cambian la página de inicio del navegador. Con frecuencia, el adware forma parte de un paquete junto con programas de distribución gratuita, lo que les permite a sus creadores cubrir los gastos del desarrollo de las aplicaciones (normalmente útiles).

El adware no constituye un peligro en sí mismo: solo puede llegar a molestar a los usuarios con las publicidades. El peligro reside en el hecho de que el adware también puede realizar funciones de seguimiento (al igual que el spyware).

Si decide usar un producto de distribución gratuita, preste especial atención durante su instalación. Lo más probable

es que el programa de instalación le informe acerca de la instalación de un programa de adware adicional. En muchas ocasiones, se le permitirá cancelar esa opción e instalar el programa sin el adware.

Sin embargo, otros programas no se instalarán sin el adware o sus funciones serán limitadas. Esto significa que el adware a menudo puede obtener acceso al sistema en forma “legal”, ya que los usuarios dieron su consentimiento para instalarlo. En este caso, es mejor prevenir que lamentarse. Si se detecta un archivo como adware en el equipo, se recomienda eliminarlo, ya que existe una gran probabilidad de que contenga códigos maliciosos.

5.1.6 Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento o el conocimiento del usuario. El spyware usa funciones de seguimiento para enviar diversos datos estadísticos, tales como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de las pulsaciones del teclado registradas.

Los creadores del spyware afirman que el propósito de estas técnicas es obtener más información sobre las necesidades y los intereses de los usuarios, y mejorar la orientación de las publicidades. El problema es que no existe una clara distinción entre las aplicaciones útiles y las maliciosas, y nadie puede asegurar que la información recuperada no se usará inadecuadamente. Los datos obtenidos por las aplicaciones spyware pueden contener códigos de seguridad, números de identificación PIN, números de cuentas bancarias, etc. El spyware suele estar incluido en un paquete junto a versiones gratuitas de programas del mismo creador con el objetivo de generar ingresos o como un incentivo para que el usuario luego adquiera el programa. Con frecuencia, se les informa a los usuarios sobre la presencia del spyware durante la instalación del programa para incentivarlos a reemplazar el producto por la versión paga, que no incluye spyware.

Algunos ejemplos de productos de distribución gratuita conocidos que incluyen spyware son las aplicaciones cliente de redes P2P (redes de pares). Spyfalcon o Spy Sheriff (entre muchas otras) pertenecen a una subcategoría específica de spyware: aparentan ser programas antispyware, pero en realidad ellos mismos son programas spyware.

Si se detecta un archivo como spyware en el equipo, se recomienda eliminarlo, ya que existe una gran probabilidad de que contenga códigos maliciosos.

5.1.7 Empaquetadores

Un programa empaquetador es un ejecutable de autoextracción y de tiempo de ejecución que combina distintos tipos de malware en un solo paquete.

Los empaquetadores más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo malware puede detectarse de manera diferente si se comprime con otro empaquetador. Los empaquetadores tienen la capacidad de hacer mutar sus “firmas” con el tiempo, lo cual dificulta mucho más la detección y eliminación del malware.

5.1.8 Bloqueador de exploits

El bloqueador de exploits está diseñado para fortalecer las aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico o los componentes de MS Office. Controla el comportamiento de los procesos en busca de actividad sospechosa que pueda indicar un exploit. Agrega otra capa de protección, acercándose a los atacantes, mediante una tecnología completamente diferente en comparación con las técnicas que se centran en la detección de archivos maliciosos en sí mismos.

Cuando el Bloqueador de exploits identifica un proceso sospechoso, puede detener el proceso inmediatamente y registrar los datos acerca de la amenaza, que se envían al sistema de la nube ESET LiveGrid. El laboratorio de amenazas de ESET procesa los datos y los usa para proteger mejor a los usuarios frente a amenazas desconocidas y ataques zero-day (malware recientemente lanzado para el que no hay una solución configurada previamente).

5.1.9 Exploración de memoria avanzada

La Exploración de memoria avanzada trabaja en conjunto con el [Bloqueador de exploits](#) para brindar una mejor protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. En los casos en los que la emulación o la heurística ordinarias no detectan una amenaza, la Exploración de memoria avanzada puede identificar un comportamiento sospechoso y buscar amenazas cuando se manifiestan en la memoria del sistema. Esta solución es efectiva contra el malware severamente ofuscado. A diferencia del Bloqueador de exploits, este es un método posterior a la ejecución, lo que significa que existe un riesgo de que se haya realizado alguna actividad maliciosa antes de la detección de una amenaza. Sin embargo, en caso de que hayan fallado otras técnicas de detección, ofrece una capa adicional de seguridad.

5.1.10 Aplicaciones potencialmente no seguras

Existen muchos programas legítimos cuya función es simplificar la administración de equipos en red. Sin embargo, en manos equivocadas, pueden ser usados con propósitos malintencionados. ESET Mail Security brinda la opción de detectar dichas amenazas.

Aplicaciones potencialmente no seguras es la clasificación usada para programas comerciales y legítimos. Esta clasificación incluye programas tales como herramientas de acceso remoto, aplicaciones para adivinar contraseñas y [registradores de pulsaciones](#) (programas que registran las pulsaciones del teclado por parte del usuario).

Si descubre que hay una aplicación potencialmente no segura presente y activa en su equipo (que usted no instaló), consulte a su administrador de red o elimine la aplicación.

5.1.11 Aplicaciones potencialmente no deseadas

Las aplicaciones potencialmente no deseadas (PUA) no tienen necesariamente la intención de ser malintencionadas, pero pueden afectar el rendimiento de su equipo en forma negativa. Dichas aplicaciones suelen requerir el consentimiento del usuario previo a la instalación. Si están presentes en el equipo, el sistema se comporta de manera diferente (al compararlo con el estado previo a su instalación). Los cambios más significativos son:

- Nuevas ventanas nunca antes vistas (ventanas emergentes, anuncios)
- Activación y ejecución de procesos ocultos
- Incremento en el uso de los recursos del sistema
- Cambios en los resultados de las búsquedas
- La aplicación establece comunicaciones con servidores remotos

5.2 Correo electrónico

El correo electrónico (o email) es una forma moderna de comunicación que tiene muchas ventajas. Es flexible, rápido y directo, y desempeñó un papel crucial en la proliferación de Internet a principios de la década de 1990.

Lamentablemente, debido a su alto grado de anonimato, el correo electrónico e Internet dejan un margen para las actividades ilegales como el envío de spam. El spam incluye avisos no solicitados, mensajes falsos y la proliferación de software malicioso (o malware). La desventaja y el peligro para el usuario se ven incrementados por el hecho de que el costo de enviar spam es mínimo y de que los creadores de spam cuentan con muchas herramientas para obtener nuevas direcciones de correo electrónico. Por otro lado, el volumen y la diversidad del spam lo hacen muy difícil de controlar. Cuanto más se use una dirección de correo electrónico, hay más probabilidades de que termine en la base de datos de un motor de spam. Algunos consejos para la prevención:

- Si es posible, no publique su dirección de correo electrónico en Internet
- Solo dé su dirección de correo electrónico a personas de confianza
- Si es posible, no use alias comunes; con alias más complejos, hay menos probabilidades de realizar un seguimiento
- No conteste los mensajes de spam que ya llegaron a su buzón de entrada

- Sea precavido al completar formularios de Internet; tenga un cuidado especial con opciones como “Sí, deseo recibir información.”
- Use direcciones de correo electrónico “especializadas”; por ejemplo, una para el trabajo, otra para comunicarse con las amistades, etc.
- De cuando en cuando, cambie su dirección de correo electrónico
- Use una solución antispam

5.2.1 Anuncios

Los anuncios por Internet constituyen una de las formas de publicidad de crecimiento más rápido. Sus principales ventajas de marketing son los costos mínimos y el alto nivel de direccionamiento; además, los mensajes se distribuyen casi de inmediato. Muchas empresas usan herramientas de marketing por correo electrónico para comunicarse en forma efectiva con sus clientes actuales y potenciales.

Este tipo de publicidad es legítima, ya que el destinatario puede estar interesado en recibir información comercial sobre ciertos productos. No obstante, muchas empresas envían mensajes comerciales masivos no solicitados. En esos casos, la publicidad por correo electrónico cruza la línea y se convierte en spam.

La cantidad de correo electrónico no solicitado comenzó a ser un problema y no muestra signos de desacelerar. Los creadores de los correos electrónicos no solicitados suelen tratar de disfrazar el spam, haciéndolos pasar por mensajes legítimos.

5.2.2 Mensajes falsos

Un mensaje falso (o hoax) es información falsa que se propaga por Internet. Los mensajes falsos generalmente se envían a través del correo electrónico o de herramientas de comunicación como ICQ y Skype. El mensaje en sí suele ser una broma o una leyenda urbana.

Los mensajes falsos propagados por virus informáticos tienen el propósito de provocar miedo, incertidumbre y duda en los destinatarios, haciéndoles creer que un “virus no detectable” presente en su equipo está borrando archivos y recuperando contraseñas, o realizando otras actividades perjudiciales para el sistema.

Para perpetuarse, algunos mensajes falsos le piden al destinatario que los reenvíen a sus contactos. Hay una gran variedad de mensajes falsos: los transmitidos por telefonía móvil, pedidos de ayuda, personas que ofrecen enviarle al destinatario dinero desde el exterior, etc. Es prácticamente imposible determinar el propósito de su creador.

Cuando un mensaje instiga al destinatario a reenviarlo a todos sus conocidos, es muy probable que se trate de un mensaje falso. Existen muchos sitios web en Internet para verificar si un correo electrónico es legítimo. Antes de reenviar dichos mensajes, el usuario debe realizar una búsqueda en Internet sobre todos los que sospeche que puedan ser falsos.

5.2.3 Phishing

El término phishing define una actividad criminal que usa técnicas de ingeniería social (manipula a los usuarios para obtener información confidencial). Su propósito es obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc.

Muchas veces logran el acceso mediante el envío de correos electrónicos encubiertos como correos legítimos de personas o empresas confiables (por ejemplo, una institución financiera, una compañía de seguros, etc.). El correo puede parecer realmente genuino y suele incluir gráficos y contenidos tomados originalmente de la fuente real por la que se hace pasar. Le solicita al usuario que ingrese, por diversas excusas (verificación de datos, operaciones financieras), ciertos datos personales, como números de cuentas bancarias, nombres de usuario y contraseñas, etc. Si ingresa estos datos, pueden ser robados y malversados con facilidad.

Hay que tener en cuenta que los bancos, compañías de seguros y otras empresas legítimas nunca solicitarán nombres de usuario o contraseñas en un correo electrónico no solicitado.

5.2.4 Reconocimiento de fraudes de spam

En general, existen varios indicadores que ayudan a identificar mensajes de spam (correo no solicitado) en su buzón de entrada. Si el mensaje cumple con al menos alguno de los siguientes criterios, probablemente se trate de un mensaje de spam:

- La dirección del remitente no pertenece a una persona de su lista de contactos
- Se le ofrece una gran cantidad de dinero, pero antes usted tiene que enviar una pequeña cantidad
- Le solicitan que ingrese, por diversas excusas (verificación de datos, operaciones financieras), ciertos datos personales, como números de cuentas bancarias, nombres de usuario y contraseñas, etc.
- Está escrito en un idioma extranjero
- Le ofrecen que adquiera un producto en el que usted no está interesado. Si igual lo desea comprar, antes verifique que el remitente del mensaje sea un proveedor confiable (consulte al fabricante original del producto)
- Algunas palabras tienen errores de ortografía para engañar el filtro del programa antispam. Por ejemplo, “vaigra” en lugar de “viagra”, etc.

5.2.4.1 Reglas

En el contexto de las soluciones antispam y los clientes de correo electrónico, las reglas son herramientas para manipular funciones de correo electrónico. Consisten en dos partes lógicas:

- 1) Condición (por ejemplo, un mensaje entrante de una dirección determinada)
- 2) Acción (por ejemplo, eliminación del mensaje, moviéndolo a una carpeta específica)

La cantidad y combinación de reglas varía según la solución antispam. Estas reglas sirven como medidas contra el spam (correo electrónico no solicitado). Ejemplos típicos:

- Condición: Un mensaje de correo electrónico entrante contiene algunas palabras que normalmente aparecen en los mensajes de spam 2. Acción: Eliminar el mensaje
- Condición: Un mensaje de correo electrónico entrante contiene un archivo adjunto con una extensión .exe 2. Acción: Eliminar el archivo adjunto y enviar el mensaje al buzón de correo
- Condición: Llega un mensaje de correo electrónico entrante enviado por su jefe 2. Acción: Mover el mensaje a la carpeta “Trabajo”

Es recomendable usar una combinación de reglas en programas antispam para facilitar la administración y filtrar el spam de manera más eficaz.

5.2.4.2 Filtro bayesiano

El filtro bayesiano para spam es una forma efectiva de filtrado de correo electrónico usada por casi todos los productos antispam. Tiene la capacidad de identificar el correo electrónico no solicitado con un alto grado de precisión y puede funcionar en forma individual para cada usuario.

Esta funcionalidad se basa en el siguiente principio: En la primera etapa, se lleva a cabo el proceso de aprendizaje. El usuario marca en forma manual una cantidad suficiente de mensajes como mensajes legítimos o como spam (en general, 200 y 200). El filtro analiza ambas categorías y aprende, por ejemplo, que el spam generalmente contiene las palabras “rolex” o “viagra” y que los mensajes legítimos son los que envían los miembros de la familia o desde las direcciones que se encuentran en la lista de contactos del usuario. Siempre y cuando se procese una cantidad suficiente de mensajes, el filtro bayesiano será capaz de asignarle a cada mensaje un “índice de spam” específico con el objetivo de determinar si es spam o no.

La ventaja principal del filtro bayesiano es su flexibilidad. Por ejemplo, si el usuario es biólogo, todos los correos electrónicos entrantes relacionados a la biología o a ámbitos de estudio afines por lo general recibirán un índice de probabilidad menor. Si un mensaje incluye palabras que normalmente corresponderían a mensajes no solicitados, pero que se envió desde una dirección incluida en la lista de contactos del usuario, se marcará como legítimo, ya

que los remitentes de la lista de contactos disminuyen la probabilidad general de que el mensaje sea spam.

5.2.4.3 Lista blanca

En general, una lista blanca es una lista de elementos o personas aceptados o que tienen acceso permitido. El término “lista blanca de correos electrónicos” representa una lista de contactos de quienes el usuario desea recibir mensajes. Dichas listas blancas se basan en palabras clave que se buscan en las direcciones de correo electrónico, nombres de dominio o direcciones IP.

Si una lista blanca funciona en “modo exclusivo”, los mensajes provenientes de cualquier otra dirección, dominio o dirección IP no se recibirán. Por el contrario, si no está en modo exclusivo, dichos mensajes no se eliminarán; se filtrarán de alguna otra forma.

La lista blanca se basa en el principio opuesto que la [lista negra](#). Las listas blancas son relativamente fáciles de mantener, mucho más sencillas que las listas negras. Es recomendable el uso tanto de la lista blanca como de la negra para filtrar el spam de manera más eficiente.

5.2.4.4 Lista negra

En general, una lista negra es una lista de elementos o personas no aceptados o prohibidos. En el mundo virtual, es una técnica por medio de la cual se aceptan los mensajes provenientes de todos los usuarios que no figuran en dicha lista.

Hay dos tipos de listas negras. Las creadas por los usuarios desde su aplicación antispam y las profesionales, que son listas negras actualizadas regularmente y creadas por instituciones especializadas, que se pueden descargar desde Internet.

Es imprescindible usar listas negras para bloquear el spam satisfactoriamente, pero es difícil mantenerlas, ya que todos los días aparecen nuevos elementos para bloquear. Es recomendable usar a la vez una [lista blanca](#) y una lista negra para filtrar el spam de la manera más eficaz.

5.2.4.5 Control desde el servidor

El control desde el servidor es una técnica para identificar correos electrónicos masivos basándose en la cantidad de mensajes recibidos y en la reacción de los usuarios. Cada mensaje deja una “huella” digital única en el servidor según el contexto del mensaje. Se trata de un número único de identificación que no revela nada sobre el contenido del correo electrónico. Dos mensajes idénticos tendrán la misma huella, mientras que dos mensajes diferentes tendrán huellas distintas.

Cuando un mensaje se marca como spam, su huella se envía al servidor. Si el servidor recibe otras huellas idénticas (correspondientes a cierto mensaje de spam), la huella se guarda en la base de datos con huellas de spam. Al analizar los mensajes entrantes, el programa envía las huellas de los mensajes al servidor. El servidor devuelve información sobre las huellas correspondientes a los mensajes que ya fueron identificados por los usuarios como spam.